Removable Media Policy

SUMMARY:

This policy sets out a best practice guidance on the use of Removable Media. When it is and is not appropriate to use removable media and how such media should be used.

This policy is meant to ensure that all users with a requirement to regularly use removable media are issued with devices and or software to facilitate the secure storage, transportation and access to data held on removable media.

1. **Purpose**

1.1. This document sets out the Policy on the use of Removable Media for the handling of information held or processed by, or on behalf of INA Prime Solutions. Information and data are critical to the realization of INA's objectives. They are also subject to protection under legislation, regulation and in accordance with the risk appetite of INA Prime Solutions.

1.2. Removable Media represents a specific vulnerability in that significant amounts of data can be held on a single item that is highly portable and easily lost or stolen. With this in mind, INA Prime Solutions has decided to **deactivate the removable storage access of each employee's computer to such devices as USB drives**. If a removable media is required and access is granted by the IT department, through this Policy the company will make every intent to:

- ensure the end-to-end security of data held and processed within INA through ensuring adequate controls;
- enhance the secure handling of information and data between INA and partners or third parties;
- help to reduce risk regarding the removal or loss of data held or processed by INA

2. **Scope**

2.1. This Policy includes, but is not limited to, the following Removable Media:

- CDs;
- DVDs;
- optical Disks;
- external Hard Drives;
- USB Memory Sticks (also known as pen drives or flash drives);
- media card readers;

- embedded microchips (including smart cards and mobile phone sim cards);
- MP3 players;
- digital cameras;
- backup cassettes;
- audio tapes (including Dictaphones and answering machines);
- smart phones when connected via USB or Bluetooth;
- fitness devices when connected via USB or Bluetooth.

3. **Applicability**

3.1. This Policy applies to all INA Prime Solutions staff (full or temporary) or any individual carrying out work on behalf of INA as well as third parties and suppliers. Suppliers are expected to follow this approach unless specifically excluded or where conditions have been applied within the procurement and contract management process.

4. **Terminology**

Term	Meaning / Application
SHALL	This term is used to state a **mandatory** requirement of this Policy
SHOULD	This term is used to state a **recommended** requirement of this Policy
MAY	This term is used to state a **operational** requirement of this Policy

5. **Policy**

5.1. The main uses of Removable Media are:

- data transfer, such as between internal systems; between networked systems and portable or mobile devices owned by INA; and between INA and third parties;
- data storage – for example the use of CDs for records and archiving.

5.2. The use of Removable Media (CDs) for the purposes of record and data storage is set out in the "*Data Retention Policy"* and the "*Personal Data Storage and Disposal Policy"*.

5.3. The portability of Removable Media also brings risk of loss or theft, therefore the exchange of data either internally or with external parties should always be via INA's information systems where possible.

5.4. Removable Media for data transfer shall only be used when all other options have been exhausted and only with the explicit permission of the General Manager of the IT department or the VP of Technology and Operations.

5.5. The use of Removable Media shall only be permitted if:

- there is a genuine business justification;
- the Removable Media is secured, appropriately authorized and as necessary, appropriately issued for holding sensitive data;
- when sending between locations, the Removable Media is sent via secure courier wherever possible or sent via a means by which it can be tracked to ensure arrival at the intended destination and by the person who has been authorized to receive it.

5.6. Personal Identifiable Information (PII) shall not be stored on or transferred to any Removable Media that is not within the control of INA Prime Solutions. Any such device shall be approved by the VP of Technology & Operations before PII is transferred onto it, and these devices shall incorporate an approved encryption technology to an appropriate standard defined in accordance with Government guidelines.

5.7. Removable Media shall be scanned and virus checked before use.

5.8. Information held on Removable Media shall be deleted once its purpose has been served and shall be documented as such by the General Manager of the IT department.

5.9. Details of information classification may be found in the "*Data Classification Policy"*. That Policy extends to Removable Media as follows:

- any Removable Media shall be classified to the highest security classification of the information stored on it;
- Removable Media shall be reclassified if the information copied onto it is of a higher classification than that currently assigned to the Removable Media, or where it is subject to a security classification upgrade.

5.10. All Removable Media shall be physically labeled with a marking that states the maximum security classification of the data held. Security classification markings on Removable Media shall be easily visually identifiable.

5.11. The safe and secure handling of Removable Media is the first level of security to prevent the unauthorized disclosure, modification, removal or destruction of information. Employees who are authorized by INA to use multimedia devices are responsible at all times for the physical security of the devices and the information held on them.

5.12. All Employees shall comply with the *"Information Security Policy"* and the *"Physical and Environmental Security Policy"* when handling Removable Media. They shall ensure the protective handling of information and the acceptable use of multimedia devices (such as Flash Memory Devices, DVDs, CDs etc.) in accordance with legislation regarding the processing of information, and the *"Acceptable Use Policy"*.

5.13. Particular care shall be taken with Removable Media that:

- holds or has held sensitive data or information; and
- is or has been connected to systems that hold or have held sensitive information.

5.14. Removable Media associated with the processing of data shall remain the property of INA Prime Solutins.

5.15. This Policy expressly prohibits the unauthorized connection of any equipment or device to INA's computer network. Employees in breach of this Policy may be subject to disciplinary procedures.

5.16. Any security breach as a result of the use of Removable Media - including loss, theft or other incident, shall be reported to the VP of Technology and Operations in keeping with the *"Information Security Policy".* The escalation route should first involve the Employee's line manager and the IT Help Desk who must also be informed.

5.17. Removable Media shall be correctly disposed of / destroyed at the end of its required lifecycle in accordance with Government guidelines and should be documented as such. Details are set out in the *"Personal Data Storage and Disposal Policy"*.

5.18. Where multiple items are held for destruction, the risk of aggregation should be taken into account, which can cause large numbers of non-sensitive items to become sensitive.

6. **Monitoring and Evaluation**

6.1. This Policy shall be reviewed every year or in response to significant changes due to security incidents, variations of law and/or changes to organizational or technical infrastructure.

6.2. This Policy is written and maintained by the VP of Technology and Operations. Questions relating to its content or application should be addressed with the VP of Technology and Operations who is responsible for facilitating communication of this Policy throughout the organization.

6.3. An Employee found to have breached this Policy may be subject to the INA's disciplinary and capability procedures and, in certain circumstances, legal action may be taken. Failure of a supplier or contractor to comply with this Policy may result in the immediate cancellation of a contract.

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