Disposal and Destruction Policy

Version 3.0

12th February 2020

Rue des Oursins, 21731, Baie du Tombeau I T : +(230) 206 8200 I F : +(230) 247 1010 I E : corporate@lasentinelle.mu

Document History

Created by:	Eddy Lareine
Approved by:	Areff Salauroo

Release date	Version	Change Details	Reviewed by
22.10.19	1.0	Submitted for review	Legal Advisor
12.11.19	2.0	Apply changes submitted by legal advisor	Eddy Lareine
12.02.20	3.0	Submitted for review	Areff Salauroo

Table of Contents

1.0 Objective *4*

2.0 Scope *4*

3.0 References to IS0 27001:2013 ..... *4*

4.0 Definitions *5*

5.0 Policy Description *5*

5.1 Management of Removable Media 5

5.2 Disposal of Media 6

5.3 Physical Media in Transit 7

5.4 Handling of Assets 8

5.5 Secure Disposal or Re-Use of Equipment 8

6.0 Enforcement *9*

7.0 Employee Declaration *9*

DISPOSAL AND DESTRCUTION POLICY

1.0 Objective

The objective of this policy is to prevent unauthorized disclosure, modification, removal or destruction of information stored on removable media including hard disks from servers, personal computers, laptops, backup tape device, pen drives, or other media holding sensitive company information.

2.0 Scope

This policy applies to all removable media of La Sentinelle Ltd holding company information.

3.0 References to IS0 27001:2013

- **Management of Removable Media - A.8.3.1**

  Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.

- **Disposal of Media - A.8.3.2**

  Media shall be disposed of securely when no longer required, using formal procedures.

- **Physical Media in Transit - A.8.3.3**

  Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

- **Handling of Assets - A.8.2.3**

  Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

- **Secure Disposal or Re-Use of Equipment - A.11.2.7**

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

4.0 Definitions

1. Removable Media include tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media.
2. System documentation refers to documentation that contains descriptions of applications, processes, procedures, data structures and authorization processes.

5.0 Policy Description

5.1 Management of Removable Media

1. Removable media is only used for business related activities to temporarily store and transport working copies of information or data, and only where no reasonable and practical alternative (such as remote access) is available.

2. All working copies of information or data on removable media devices are adequately protected, according to its assessed need for confidentiality, integrity and availability commensurate with the information's value.

3. The following guidelines for the management of removable media are applied by La Sentinelle Ltd:

    (i) If no longer required, the contents of any re-usable media that are to be removed from La Sentinelle Ltd, are made unrecoverable. Previous contents of re-usable media are erased and the erasure applies across the totality of the media, not simply across what appears to be the existing content to prevent leakage of information to unauthorized persons. Prior authorization is required before erasing the contents of any media. This is recorded on a ***Media Removal Form.***

    (ii) Where necessary and practical, authorisation is required for media removed from La Sentinelle Ltd and a record of such removals is kept in order to maintain an audit trail. Certain media such as back up tapes are

removed from La Sentinelle Ltd premises (Data Centres) daily for transfer to offsite locations & tape rotations, while others such as a hard disk containing specific information may leave La Sentinelle Ltd premises on specific occasions. All movements of removable media are recorded on a ***Media Movement Form.***

(iii) All media are stored in a safe, secure environment, in accordance with manufacturers' specifications.

(iv) Information stored on media that needs to be available longer than the media lifetime (in accordance with manufacturers' specifications) is transferred to another media and stored in appropriate locations in order to avoid information loss due to media deterioration.

(v) Removable media drives are only enabled if there is a business reason for doing so.

5.2 Disposal of Media

1. When no longer required, media is disposed of securely and safely and according to applicable legislation and formal procedures, to minimize the risk of sensitive information leakage to unauthorized persons.

2. Each type of media needs different disposal methods and the procedure for secure disposal of media containing sensitive information is commensurate with the sensitivity of that information.

(i) Disposal of Damaged or Inoperable Hard Drives

The owner must first attempt to overwrite the hard drive. If the hard drive cannot be overwritten, the hard drive must be disassembled and mechanically damaged so that it is neither usable nor readable.

(ii) Disposal of Electronic Media Outside of La Sentinelle Ltd

All electronic media other than computer hard drives are erased, degaussed, or rendered unusable before leaving La Sentinelle Ltd premises.

(iii) Disposal of Paper Records

Paper records containing sensitive information are disposed of by shredding them so that they cannot be recovered.

5.3 Physical Media in Transit

1. Security of media being transported beyond La Sentinelle Ltd boundaries is of utmost importance to protect them from unauthorized access, misuse or corruption.

2. Back up tapes are transported daily from one site to another. Other types of media such as external drives are also transported withing La Sentinelle Ltd physical locations/sites whenever applicable.

3. The following guidelines are taken into consideration to protect media in transit between sites:

    i. Physical media containing backup data are transported in a protective bag to protect them from environmental damage such as excessive heat, moisture or electromagnetism.

    ii. Only authorized La Sentinelle Ltd staff is allowed to transport physical media containing data backup between the different premises.

    iii. Receipt and delivery of data tapes are recorded and reviewed on a regular basis.

    iv. Where applicable, sealed envelopes are used to deliver physical media.

    v. After delivery, verifications are performed (e.g. by phone) to confirm whether recipient has indeed received the correct media.

    vi. Security incidents are reported and appropriate action taken. (e.g. in case seals are broken in transit).

5.4 Handling of Assets

1. Information should be properly handled and stored to protect from unauthorized disclosure or misuse.

2. All handling, processing, storage and communication of information should be consistent with its classification as per ***Clause- Information Handling and Labeling of the Asset Policy.***

3. The following guidelines are applied to protect information from unauthorized disclosure or misuse:

   i. Access to media containing information is restricted to authorized personnel only.
   ii. A formal record of authorized recipients of information is maintained and regularly updated.
   iii. It is ensured that :

      a) Input data is complete;
      b) Processing is properly completed;
      c) Output validation is applied;
      d) Spooled data awaiting output is also protected depending on its sensitivity;
      e) Media is stored in accordance with manufacturers' specifications;

5.5 Secure Disposal or Re-Use of Equipment

All items of equipment containing storage media are checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Devices containing sensitive information are physically destroyed or the information destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Whenever devices containing sensitive data are damaged, a risk assessment is carried out to determine if device should be physically destroyed rather than sent for repairs or discarded.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Employee Declaration

I have read and I understand the above Disposal and Destruction Policy, and consent to adhere to the rules outlined therein.

Name : _____

Signature : _____

Date : _____