

ASSET (MEDIA/EQUIPMENT/SOFTWARE) HANDLING PROCESS

**Version History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver.** | **Date** | **Description of Change** | **Author** | **Reviewed By** | **Approved By** |
| 0.1 | 3rd Sep 13 | First Draft | Saket Madan | Dhananjay kumar | Ajay Kr. Zalpuri |
| 1.0 | 31st Oct 13 | Approved and Baselined | Saket Madan | Dhananjay kumar | Ajay Kr. Zalpuri |
| 1.1 | 29th July 2015 | **To meet the new requirement of ISO 27001:2013 clause A 12.6.2 has been modified in section 7. Guidelines for Desktop/Laptop/Server users** | Rahul Raj | Dhananjay kumar | Ajay Kr. Zalpuri |

**Table of Contents**

[1. Objective 4](#_Toc373847519)

[2. Scope 4](#_Toc373847520)

[3. Access and Ownership 4](#_Toc373847521)

[4. Asset (Media/Equipment/Software) Labeling 4](#_Toc373847522)

[5. Transportation of Asset (Media/Equipment/Software) 4](#_Toc373847523)

[6. Disposition 5](#_Toc373847524)

[7. Guidelines for Desktops and Laptops users 5](#_Toc373847525)

# Objective

The purpose of this document is to explain policy for preventing unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

# Scope

This policy applies to all Asset (Media/Equipment/Software) including hardware and physical Asset (Media/Equipment/Software) that might contain organizational data. Sensitive data includes but is not limited to, tapes, disks, CDs, paper and any print or electronic data.

# Access and Ownership

* Sensitive data, for example, network diagrams, list of server configurations etc. shall only be given to those employees with a need to know and who have authorized access in the performance of their official duties.
  1. Sensitive information must not be left unattended, even temporarily
  2. Sensitive data must remain in an authorized employee’s physical [control](http://www.t2pa.com/component/glossary/Policy-Glossary-1/I/Internal-Control-28/) at all times
  3. Sensitive information being hand-carried must be kept with the individual and protected from unauthorized disclosure.
* Physical, environmental protection controls shall be provided for sensitive data contained in a Asset (Media/Equipment/Software) storage vault or library.

# Asset (Media/Equipment/Software) Labeling

* All data and information that is sensitive should be dated and marked.
* External labeling shall include any special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)

# Transportation of Asset (Media/Equipment/Software)

All Asset (Media/Equipment/Software) transported out of the company premises or between buildings would be accompanied with a Gate Pass and a copy would be maintained at the sending gate. The Gate Pass would contain information about the Asset (Media/Equipment/Software) asset being sent out, the name of the person carrying it along with his/her contact information, the receiving person’s details and the person who has approved the transportation of the asset.

The Asset (Media/Equipment/Software), transported through postal or [vendor](http://www.t2pa.com/component/glossary/Policy-Glossary-1/V/vendor-51/) services, shall be secured using the following procedure:

* + Bar Code/ Sl.No. or any other confidential information is maintained in gate pass
  + Receipt and delivery of sensitive data must be monitored and accounted for to ensure that data is not lost and potentially compromised while in transit.

# Disposition

* All magnetic storage Asset (Media/Equipment/Software) that contains sensitive data must be sanitized when it is no longer needed to store sensitive data.
* Software overwrite procedures may be used as an alternative.
* While returning any leased machines, IT would ensure that the Hard disk is formatted (low level formatting).
* Non-functioning and/or non-writable Asset (Media/Equipment/Software) containing sensitive data should be completely formatted. If it is not possible the Asset (Media/Equipment/Software) should be physically destroyed prior to disposal so that data will not be retrieved and reused.
* If hard drive of servers and sensitive PC develop bad sectors and become un-repairable. The supplier of the server shall replace the faulty disk and IT dept shall ensure that it is properly sanitized before finally disposed off by the supplier.
* A list of disposal Asset (Media/Equipment/Software) shall be maintained

# Guidelines for Desktop/Laptop/Server users

* All passwords should conform to the guidelines in password policy. Users should avoid storing passwords or other information that can be used to gain access to other computing resources.
* Users should not run any unauthorized or undocumented software on their desktops. IT department will approve on the recommendation of Department Heads, the installation of any software on Desktop/Laptop/Servers.
* Users should not share the folder on their PC without password and in full access mode as someone can delete or modify the existing files in shared directory. Cases must be raised in incident log (Incident management), where someone has copied unwanted/objectionable files in shared directory. Whenever required, sharing should be done in ‘READ ONLY’ mode.
* User should not install and play computer games on PC.
* User should maintain following Guidelines while carrying any Laptop:
  + Important & sensitive business data in Laptop should be encrypted when it is taken outside the organization.
  + Latest Patches & updates should be installed in the Laptop.
* Laptop entry should be maintained on reception while brought from outside and should be scanned for virus before connecting to organizational network.