BESSEGGEN INFOTECH LLP

Information and Cyber Security Framework

INFORMATION ASSET MANAGEMENT POLICY & PROCEDURES

Reference No.: BESSEGGEN/I&CSF/AM
Version: 1.2

30th May 2025

Internal Use Only

Document Control			
Reference No.	BESSEGGEN/I&CSF/AM		
Document Name	**BESSEGGEN – Information Asset Management Policy & Procedures**		
Version No.	1.2		
Document Status	Definitive		
Issue Date	30th May 2025		
Compliance Status	Mandatory		
Review Period	One year from the date of release or earlier if required		
Security Classification	Internal Use Only		
Distribution	Part of BESSEGGEN I&CSF		
	Name	**Role**	**Signature**
Authored by	BESSEGGEN INFOTECH LLP		
Reviewed by	Prince Kumar	Developer	
Approved by	Vibhu Garg	CISO	
Released by	BESSEGGEN INFOTECH LLP		

Document Revision History		
Version	**Release Date**	**Change Description**
1.0	08th Aug 2022	Issued
1.1	13th May 2024	Reviewed
1.2	30th May 2025	Reviewed

Table of Contents

1. Overview

The Asset Management Policy and Procedures of BESSEGGEN INFOTECH LLP (henceforth named as "BESSEGGEN") ensure the effective management of assets used in the organization's processes, systems, and services to meet the business and information security requirements.

2. Objectives

BESSEGGEN provides guidelines for the identification, classification, ownership, handling, and protection of assets against unauthorized access, loss, theft, damage, or misuse.

- To ensure that all assets are adequately protected through the implementation of security measures that align with business and information security requirements.
- To ensure that all assets are handled, stored, and disposed of appropriately and securely in compliance with legal, regulatory, and contractual obligations.

3. Scope

This policy applies to all BESSEGGEN employees, Third party vendor, and clients. This policy outlines the framework and approach to the management of assets within BESSEGGEN. as mandated by the Regulatory agencies SEBI, CERT-IN and ISO 27001:2013

4. Policy Statement:

In managing the assets belonging to BESSEGGEN, we are committed to:

- Ensuring decisions are made during all life-cycle stages and interrelationships between asset, operational and service performance.
- Reviewing this policy and making any necessary adjustments on an annual basis

Refer: Asset Management Control guidelines stated as per Appendix-C Asset Management Controls ISO 27001:2013

5. Terms used and Definition:

SN	Terms	Definitions
1	**Guidelines**	To identify how physical and logical security will be provided for hardware and software assets (locks, passwords, virus protection, etc.).
2	**Licensing**	To keep track of asset licensing, ensuring compliance with all relevant agreements, laws and regulations.
3	**Asset Management**	Asset Management is which employs predictive modelling, risk management and optimized decision-making techniques to establish asset lifecycle treatment options and related long term cash flow predictions.
4	**Asset**	An asset is an object (physical or intangible) that has an identifiable value and a useful life greater than 12 months, that is or could be used by the entity responsible for it to provide a service.

5	**Criticality**	Criticality is the quality, state, or degree of being of the highest importance
6	**Economic value**	The Economic value of an asset is the length of time for which maintaining and operating the asset remains the lowest cost alternative for providing a nominated level of service.
7	**System**	An equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, control, display, switching, interchange, transmission or reception of data and that includes computer software, firmware and hardware.
8	**Threat**	A potential to cause an unwanted incident which may result in harm to a system such as unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin
9	**Non-Disclosure Agreements (NDA)**	A legally binding document which protects the confidentiality of ideas, Designs, plans, concepts, or other commercial material.
10	**Threat**	An intention or a determination to inflict harm (or something Unpleasant) on an Information Asset.
11	**Security breach**	Violation of any security policy or procedures.
12	**Software**	Generic term used for Operating systems, firmware, databases, web servers, applications, services / daemons, drivers etc.
13	**Source Code**	The actual program, as written by the programmer, which is compiled into machine code which the computer can understand.
14	**Policy**	An overall declaration of management intent for information security. It states what needs to be done to foster information security goals and objectives of BESSEGGEN. It contains managerial, technical, operational, and physical security control measures that are commensurate with The information assets being protected.
15	**Remote Access**	Ability to get access to a computer or a network from a remote Distance.
16	**Network**	A configuration of communication equipment and communication links by network cabling or satellite, which enables computers and their terminals to be geographically separated, while still connected to Each other.
17	**Information Security**	A process of safe-guarding information assets from unauthorized access, modification, use, disruption, and destruction to ensure confidentiality, integrity, availability, and non-repudiation of information.
18	**Information Security Event**	An event that is caused due to any action on an Information Asset. For example, deleting a key file from a critical business system.
19	**Information Security Incident**	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
20	**Intrusion**	An uninvited and unwelcome entry into a system by an unauthorized source.
21	**Key Management**	In cryptography, it is the creation, distribution, and maintenance of a secret key. It determines how secret keys are generated and made available to both parties; for example, public key systems are widely used for such an exchange. If session keys are used, key management is responsible for generating them and determining when they should be renewed

6. Roles and Responsibilities:

SN	Roles	Responsibilities
1	CISO	To establish policy so that it protects people, assets, infrastructure and technology.
2	IST Ambassador	Coordinate the activities not only within organization as well with external bodies for information's security standards and guidelines related updates.
3	Manager Compliance	Coordinate with regulatory and government agencies for information security standards, guidelines compliance and audit processes.
4	Manager Security Operations	Information security managers are responsible for ensuring that all security programs, tools, and technologies are working correctly, as well as providing the necessary protections to the company's networks, digital communications, and databases
5	Manager ISPP	Conduct regular audits of policies, procedures and controls to make sure they are being adhered to standards as per regulatory authorities.
6	IT Head	Lead, manage, and govern the information assets are adequately protected, safely guarded and disposed-off as per data security guidelines and regulatory requirements.
7	Head Finance	Creating forecasting models, assessing risk in investments and ensuring all accounting activities comply with regulations.
8	HR Head	For leading and ensuring assets are returned back after the exit of an employee, termination, or transfer to different business units in the organization.
9	BU Head	Lead, manage, and govern the acquisition and application of assets within the business unit of the organization.
10	BU SPOC	Works closely with teams to harvest potentially reusable assets and to integrate existing assets into their work. May also develop, evolve, support, and retire assets.

7. Asset Management Guidelines and Procedure:

7.1 Responsibility of Assets

Objective is to identify assets and define protection responsibilities.

7.1.1 Inventory of Asset

A comprehensive information asset register/ inventory will be drawn for all types of assets to keep track of the location and record keeping.

- **Information Asset:** Employee information, Magnetic media (tapes and disks), system documentation, user manuals, training material, operational and support procedures, daily routine logs, third party contracts, network architecture documents etc.
- **Hardware Assets and Infrastructure Facilities:** Data Centre, Computer hardware (Servers, desktops, laptops, printers, Scanner etc.), network and communication equipment (routers, switches, modems, etc.), other infrastructure equipment (power supplies, air conditioning units, UPS, DG sets), furniture, etc.

- **Software Assets:** Application software, system software, database software, databases and data files, networking software, security and control software, development tools and utilities, etc.
- **People:** Employees, who hold sensitive information or have access to sensitive information and areas, shall be identified by the IT department. They shall be given information and cyber security training on the defined security controls / procedures, which they shall adhere to.

Implementation Guidelines:

- Assets should be identified and documented so that appropriate protection can be implemented.
- Asset inventory should be accurate, up to date, and consistent and aligned with owner details and relevance with other inventories.
- The inventory of the assets should record information about their business value and classification), and their backup and disaster recovery arrangements.
- The inventory of physical assets should contain full details of equipment identity, including owner, location, maker, model, generic type (e.g. printer, PC), serial number, date of acquisition and inventory tag etc.
- A record of disposals when and how or who to that also needs to be kept, and the asset inventory should be updated.
- All software products should also be listed in the asset inventory, where they are used and where the original media are kept, together with the relevant licensing information.
- Maintain an up-to-date centralized inventory of authorized SW/Application and libraries etc.
- Adequate procedures should be in place to maintain accuracy of the inventory and a stock check should be carried out at least annually.
- Use client certificates to authenticate hardware assets connecting to the BESSEGGEN network.
- The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.

7.1.2 Ownership of Asset

Assets maintained in the inventory shall be owned.

Implementation Guidelines:

- Ownership should be assigned when assets are created or when assets are transferred to the organization. The asset owner should be responsible for the proper management of an asset over the entire asset lifecycle.
- Asset owner can be either an individual or an entity. Owner does not necessarily have property rights of an asset.
- It is necessary to appoint an asset owner for all major assets, and this asset owner is responsible for the asset itself, and its protection. This includes:
    - Determining the classification of the asset.

- Supporting risk assessments by giving input about the asset's business value and its importance for the organization's business activities.
- Ensuring appropriate protection in the day-to-day use of the asset.
- Keeping security classifications and control arrangements up to date.

- As most organizations have a lot of assets and/or complex systems, it can help to consider several assets together, e.g. all assets involved in a particular business process or in the provision of a particular service. The owner of that process or service could then be responsible for all of the assets involved in the process or service, and for their correct functioning and provision.

7.1.3 Asset Provisioning and De-provisioning procedure

Provisioning of Assets

- In case of new Joiner, End-User systems (Desktops/ Laptops) will be provided by the IT Infrastructure department to any BESSEGGEN and IT department is required to provide the asset on the same date of the receiving the request and approval for the respective employee/s.
- Asset is not available then procurement of new asset/s is to be initiated by the IT Team Infrastructure department,
- The IT Infrastructure Department shall inform through email the employee once the Asset has been procured and all necessary controls are in place, to allocate the asset.
- IT Infrastructure Department shall inform the Department Head and the HR team once the Asset is allocated and the Information Asset Register shall be duly updated (as per Asset Inventory Procedure above)
- New Asset procurement requests for Servers and Network Equipment have to be requested by the IT Infrastructure Department and accompanied with proper justification of business use and budget. Requests need to be accompanied by approval of the CTO/ IT Head, as well as the BESSEGGEN Finance Department/ CFO (for budget approval)
- Allocation of Personalized peripherals will be purely based on business requirement, and IT Head/ CTO approval will be needed for the same.
- Concerned Department Heads will be responsible for the peripheral allocated to their respective Department.

De-Provisioning of Assets

- In case of employee exit/ termination the exit details and e-mail are shared by the HR department with the IT infrastructure department. Post approval from the concerned Department Head, the asset owner/ employee will hand over the asset and records are updated accordingly.
- Any asset shall stay in service for a minimum of five years. Further a complete evaluation of the asset will be carried by the IT department. The IT department shall conduct a periodic review of all assets on a half yearly basis. Old Assets identified for replacement are taken back and new assets are handed over to users post email approval from IT Head/ CISO and Finance Head (CFO).
- Information Asset Register shall be duly updated after Asset Reassignment with the reassignment

timelines and other details updated.

7.1.4 Acceptable Use of Asset

Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented, and implemented.

Implementation Guidelines:

- Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's assets.
- To ensure that assets are only used for their intended business purpose, the organization should identify, develop and implement rules, procedures and guidelines describing the acceptable use of the assets.
- It is important that everyone using the asset signs up NDA form, using the asset.

7.1.5 Return of Asset:

All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

Implementation Guidelines:

- During the notice period of termination, the organization should control the unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.
- The organization should have procedures in place to ensure that all assets in the possession of employees, contractors and third-party users are returned when their employment terminates or changes.
- All of the organization's information that might have been stored on non-organizational assets, such as private equipment, or equipment of a third-party organization or of a contractor, should also be returned and securely erased from that equipment. The return of assets should be part of the contract.

7.2 Information Classification

The objective is to ensure that information receives an appropriate level of protection in accordance with its importance and criticality to the organization.

7.2.1 Classification assets and Information

Assets and Information should be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. The asset classification for BESSEGGEN assets shall be as per below categories:

- Restricted
- Confidential
- Internal
- Public

Implementation Guidelines:

- Assets other than information can also be classified in conformance with the classification of information, which is stored in, processed by or otherwise handled or protected by the asset. Should be consistent across the whole organization so that everyone will classify information and related assets in the same way and apply for the appropriate protection.
- Owners of information assets should be accountable for their classification.
- Results of classification should indicate the value of assets depending on their sensitivity and criticality to the organization, e.g., in terms of confidentiality, integrity, and availability.
- Procedures are required to specify the handling, storage and disposal requirements of each classification.
- Also, allowance should be made for the need to reduce the level of classification if the sensitivity reduces – and vice versa. Provide for change and expiry dates in these circumstances. The asset owner should be responsible for handling and updating the classification and notification to all recipients and users.
- The Risk Management department may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at a certain classification level.

Risk Rating	Classification	Confidentiality Rating	Impact
Very Low (1)	**Public**	1	This classification applies to the information, which has been explicitly approved by the management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information, and it may be freely disseminated without potential harm.
Low (2)	**Internal**	2	This classification applies to all other information, which does not clearly fit into any of the other three classifications. While its unauthorized disclosure is against the policy, it is not expected to seriously or adversely impact the business, employees, Clients, stockholders and/ or business partners.
Moderate (3)	**Confidential**	3	This classification applies to the sensitive business information, which is intended for the use within BESSEGGEN. Its unauthorized disclosure could adversely impact the business, its stockholders, its business partners, its employees and/or its clients.

High (4)	**Restricted**	4	This classification applies to the most critical business information, which is intended strictly for the use within BESSEGGEN. Its unauthorized disclosure could adversely impact the business, its stockholders, its business partners and/ or its clients leading to the legal and financial repercussions and adverse public opinion. The information that some people would consider to be private is included in this classification.

7.2.2 Labeling of Information

An appropriate set of procedures for information labeling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Implementation Guidelines:

- All information items should be prominently labeled to ensure that they are given the necessary protection in use, storage and transport. The labeling should reflect the classification scheme established.
- The labels should be easily recognizable.
- Employees and contractors should be made aware of labeling procedures.
- Information held in information systems should also be classified and maintained in the system or application documentation. This should be reflected in the system in terms of access levels and the range of users who can access it and at what level (read-only, write, delete).
- Low sensitivity information might be sent in an open email message but information of higher sensitivity may require encryption.
- Information may cease to be sensitive after a certain period of time, e.g. when it has been made public. In such cases, provide an expiry date to avoid unnecessary protection expenses.

7.2.3 Handling of Assets

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

Implementation Guidelines:

- Disposal procedures should be proportional to the information classification level and secure disposal.
- To ensure the items were properly disposed of, you should keep log information listing, at a minimum, who performed the procedure, when, and what method was used.
- There is serious risk of a breach of confidentiality when sensitive information is being handled, e.g. invoices, cheques and financial transaction data. Additionally, breaches of integrity and availability also need consideration with regard to information assets. Procedures for the handling, processing, communication and storage of sensitive, critical or personally identifiable information, together with appropriate authorities and records, are required for the safe use of all these forms of

information.

- Where carriers or couriers are transporting the items, ensure that there is a clear record of proven identity of the individual as well as packing and sending through insurance coverages. All items should be clearly marked with the name of the ultimate recipient, who should provide a record of receipt.
- Confidentiality or non-disclosure agreements need to be in place to protect privacy of information. Sensitive or critical items should be identified by risk assessment or, in the case of personally identifiable information, by a privacy impact assessment, and all activities and movements should be logged for later monitoring.
- BESSEGGEN manages and protects data/information assets considering how the data/information are stored, transmitted, processed, accessed and put to use within/outside the BESSEGGEN network, and level of risk they are exposed to depending on the sensitivity of the data/information.
- It should be ensured that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.

Environmental Security for Assets

- Power supply is critical for uninterrupted functioning of the company. The power supply arrangements are as follows:
- A dedicated UPS and automated DG should start up as soon as the electricity supply from the local power supplier gets cut off.
- The whole premises should have air-conditioning facilities to prevent dust, heat and air pollution affecting IT equipment.
- The whole premises should be fitted with automatic fire alarms.
- The Critical Areas should ideally be fitted with a fire extinguisher.
- Smoke detectors should be located on each floor and should automatically trigger off the smoke alarm if smoke is detected.
- Protection from Floods: The premises should have adequate flood and rainwater drains. The premises should be continuously maintained to ensure that water seepage, if any, is detected and corrective action is initiated.
- Switches: Switches and sockets should all be grounded (provided with earthing) and provided with circuit-breakers to avoid any untoward occurrences due to faulty wiring or short circuits.
- Monitoring and testing is done periodically to check the performance of such deployments.

7.3 Media Handling

To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

7.3.1 Management of Removable Media

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

Implementation Guidelines:

- If no longer required, then the contents of any re-usable media that are to be removed from the organization should be made unrecoverable.
- Where necessary authorization should be required for media removed from the organization and a record of such removals should be kept in order to maintain an audit trail.
- All media should be stored in a safe, secure environment, in accordance with manufacturers' specifications.
- Data confidentiality or integrity are important considerations. Cryptographic techniques should be used to protect data on removable media.
- Removable media containing the organization's data presents a serious vulnerability to loss of data and breaches of confidentiality. Controls are required in the management of media items, which could be tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media.
- Procedures should be developed and implemented to ensure that media are used, maintained, and transported in a safe and controlled manner, based upon the classification of the information stored on the media.
- The different authorization levels should be documented. Any risk assessment should recognize that the effectiveness of controls is limited by the ease with which small media items (e.g. USB sticks) can be removed from the premises.

7.3.2 Disposal of Media

Media should be disposed of securely when no longer required, using defined procedures.

Implementation Guidelines:

- Media containing confidential information should be stored and disposed of securely. E.g. by incineration or shredding. Or erasure of data for use by another application within the organization.
- Disposal of sensitive items should be logged in order to maintain an audit trail.
- Serious breaches of confidentiality occur when apparently worthless disks, tapes, paper files and printer ribbons are dumped without proper destruction.
- The procedures for the handling of classified information should cover the appropriate means of its destruction and disposal.
- A record of sensitive items should be maintained at the point of destruction.

Disposal of Assets

- Assets which are analyzed by the IT Infrastructure team to be damaged and not repairable or obsolete are listed out.
- Approval Note is prepared, and Approval is taken from the IT head/ CTO and the Finance Head, CFO, for Asset Disposal.
- Assets are disposed as per the Media Disposal Procedure.

7.3.3 Physical Media Transfer

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

Implementation Guidelines:

- A list of authorized couriers should be agreed with management.
- Packaging should be sufficient to protect the contents from any physical damage during transit with proper insurance coverages as agreed agreements with courier services.
- Logs should be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.
- A risk assessment should be used to help select the right transport method and the controls applied to it (e.g. by post with recorded delivery, secure parcel delivery, personal delivery by trustworthy couriers).
- To significantly mitigate the risk of breach of confidentiality if media are lost or stolen, consider encryption of data to be transported; if encrypting, never ship the encryption key and/or password with the encrypted data. All dispatches should be recorded and, where appropriate, authorized.

7.3.4 Asset Theft/ Missing Management Procedure

- In case an Asset goes missing or is stolen, the Asset User needs to communicate this to the BESSEGGEN Administration and the IT Infrastructure team immediately.
- The Asset User needs to lodge a FIR/ Complaint copy from the Police for the missing/ theft cases.
- The Asset User needs to share the FIR/ Complaint copy with the BESSEGGEN Administration, IT Infrastructure and the HR Departments

7.3.5 Absconding Employee (with Asset) Management Procedure

- In case a BESSEGGEN /Third Party employee is absconding with the assigned asset, then the HR Department shall communicate the same with the IT Infrastructure Department
- The IT Infrastructure Department shall communicate the Asset Value/ Cost to the HR Department. Asset Value/ Cost shall be adjusted from the employee's Full & Final settlement by the HR Department.
- HR shall inform the IT Infrastructure Department once the Asset Value/ Cost is adjusted in the employee's Full & Final settlement.
- Information Asset Register shall be duly updated by the IT Infrastructure Department.

7.4 Exception Management

Exceptions to the guiding principles in this policy must be documented and formally approved by the CISO/Management and exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Evidence of approval by the CISO/Management

8. RACI Matrix

SN	Procedure	Description	CISO	IST Ambassador	Manager ISPP	Manager Security Operation	Head/ Manager	IT Head /	HR Head / Manage	BU-1 He	BU-1 SPOC	Target Timeline For

						s	Finance	Manager	r	ad		Compliance
1	Inventory of assets	Inventory of these assets shall be drawn up and maintained.	I	I	C	R	I	A	C	R	R	Yearly
2	Ownership of assets	Assets maintained in the inventory shall be owned.	I	I	C	I	I	A	C	R	R	Yearly
3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities are documented and conveyed.	I	I	C	I	I	A	C	R	R	Yearly
4	Return of assets	Return all of the organizational assets upon termination of the employment, contract or agreement.	I	I	C	I	I	A	R	R	R	To be reviewed Quarterly
5	Classification of Information	Asset / information classification in terms of legal requirements, criticality and sensitivity to unauthorized disclosure or modification.	I	I	C	I	I	A	C	R	R	Yearly to be reviewed
6	Labeling of information	Asset / Information labeling developed and implemented in accordance with the information classification scheme.	I	I	C	I	I	A	C	R	R	To be reviewed Quarterly
7	Handling of assets	Procedures for handling assets developed and implemented in accordance with the information classification scheme.	I	I	C	I	I	A	C	R	R	To be reviewed Quarterly
8	Management of removable media	Procedures implemented for the management of removable media in accordance with the classification scheme.	I	I	C	I	I	A	C	R	R	To be reviewed Quarterly

9	Disposal of media	Media disposed off securely when no longer required, using formal procedures	I	I	C	I	I	A	C	R	R	To be reviewed Quarterly
10	Physical media transfer	Media containing information is protected against unauthorized access, misuse or corruption during transportation.	I	I	C	I	I	A	C	R	R	

Appendix A: Information Asset Inventory:

Organisation & relevant				Information Asset Details						Information Asset Details						Purchase Information				Quality					Location		Level of protection		
SN	Operating Unit / Function	Process name	Process owner	Asset ID	Name of Asset	Description of Asset	Type of Information Asset (Hard copy, Electronic File (specify	Personal Data (Y/N)	Personal Sensitive Data (Y/N)	Sensitive Customer Data (Y/N)	Classification	Integrity	Availability	Asset Owner	Asset Custodian (if NOT Functional Owner)	Date	Supplier	Warranty expiration	Original Price	Condition	Depreciation of asset (If	Unit Val	Quantity	valu e	Department / area	Room	Data Retention Period	At Origin (description)	If Info on is Mov (desc n)
1																													
2																													
3																													
4																													

Appendix B: Disposal of Media:

SN	Asset ID	Manufacturer	Model	ORG Assisgned No.	Media Type	Disposal Confidentiality Category	Disposal Description	Disposal Method Used	Tool & Version Used	Backup Taken if needed	Verification Method	Post Disposal Destination	Name of Person	Designation	Date	Location	Co No

Appendix C: Asset Management Control ISO 27001:2013

A.8 Asset management		
A.8.1 Responsibility for assets		
Objective: To identify organizational assets and define appropriate protection responsibilities.		
A.8.1.1	Inventory of assets	*Control* Assets associated with information and information processing facilities

		shall be identified and an inventory of these assets shall be drawn up and maintained.
A.8.1.2	Ownership of assets	*Control* Assets maintained in the inventory shall be owned.
A.8.1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.
A.8.1.4	Return of assets	*Control* All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
A.8.2 Information classification		
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
A.8.2.1	Classification of information	*Control* Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
A.8.2.2	Labelling of information	*Control* An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.2.3	Handling of assets	*Control* Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.3 Media handling		
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information Stored on media.		
A.8.3.1	Management of removable media	*Control* Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
A.8.3.2	Disposal of media	*Control* Media shall be disposed of securely when no longer required, using formal procedures.
A.8.3.3	Physical media transfer	*Control* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.