ASSET MANAGEMENT POLICY

INLINE WITH ISO 27001:2022 & SOC 2

Prepared By :

MINISTRY OF MOS SECURITY

Document Name	**Asset Management Policy**
Classification	**Internal Use Only**

Document Management Information

Document Title:	Asset Management Policy
Document Number:	ORGANISATION-ACS-MNM-POL
Document Classification:	Internal Use Only
Document Status:	Approved

Issue Details

Release Date	DD-MM-YYYY

Revision Details

Version No.	Revision Date	Particulars	Approved by
1.0	DD-MM-YYYY	<Provide details of changes made on policy here>	<Provide name of Approver here>

Document Contact Details

Role	Name	Designation
Author	<Provide name of author here>	<Provide designation of author here>
Reviewer/ Custodian	<Provide name of reviewer here>	<Provide designation of reviewer here>
Owner	<Provide name of owner here>	<Provide designation of owner here>

Distribution List

Name
Need Based Circulation Only

Document Name	Asset Management Policy
Classification	Internal Use Only

CONTENTS

Document Name	Asset Management Policy
Classification	Internal Use Only

1. PURPOSE

The purpose of this Asset Management Policy is to establish a standardized framework for the identification, classification, handling, allocation, protection, and disposal of all organizational assets throughout their lifecycle. This policy ensures that assets—both physical and logical—are appropriately managed to preserve the confidentiality, integrity, and availability of [ORG NAME]'s information and infrastructure, in alignment with ISO/IEC 27001 and SOC 2 Type 2 requirements.

2. SCOPE

This policy applies to all employees, contractors, consultants, vendors, interns, and third-party entities who access, manage, or are assigned any organizational asset owned, leased, or otherwise managed by [ORG NAME].

The scope of this policy includes, but is not limited to:

- **Physical assets**: laptops, desktops, servers, networking devices, mobile devices, storage media, and office equipment.
- **Logical assets**: data, databases, software applications, licenses, digital certificates, configuration files, and intellectual property.
- **Supporting assets**: infrastructure and facilities, access badges, security tokens, and any tools that support information processing activities.

This policy is applicable across all environments where [ORG NAME] assets reside, including on-premises facilities, remote work locations, data centres, and cloud platforms.

3. TERMS AND DEFINITIONS

- **Asset**: Any item of value to the organization, including physical hardware, digital information, software, intellectual property, or supporting infrastructure used in business operations.
- **Asset Owner**: The individual or team responsible for the overall lifecycle, classification, protection, and usage of a specific asset.
- **Asset Custodian**: A designated person or team responsible for the day-to-day management and safeguarding of the asset as per the asset owner's guidelines.
- **Asset Inventory**: A comprehensive and up-to-date register of all organizational assets, including their ownership, classification, and status.
- **Classification**: The categorization of assets based on their sensitivity, value, and criticality to business operations (e.g., Public, Internal, Confidential, Restricted).
- **Valuation**: The process of determining the relative importance or financial worth of an asset, considering its impact on operations, compliance, and security.

- **Declassification**: The formal process of changing an asset's classification level to a lower sensitivity status based on revised business or risk context.
- **Allocation**: The assignment of an asset to a user, department, or function for authorized use.
- **Transfer**: The movement of an asset between users, departments, or locations with necessary approvals and updates to the inventory.
- **Disposal**: The secure and compliant removal of an asset from active use, including data sanitization and environmentally responsible destruction where required.

4. ROLES AND RESPONSIBILITIES

Role	Responsibility
Chief Information Security Officer (CISO)	Overall ownership of the Asset Management Policy. Approval of exceptions, high-risk asset classifications, and disposal of critical assets. Ensures alignment with ISO/IEC 27001 and SOC 2 requirements.
Information Security Team	Oversight and monitoring of asset classification, labelling, handling, and disposal. Conducts periodic audits, risk assessments, and ensures compliance enforcement.
IT Operations Team	Maintains and updates the asset inventory register. Executes asset allocation, reallocation, and disposal procedures. Supports tagging, labelling, and secure maintenance activities.
Asset Owners	Define classification levels, usage guidelines, and protection requirements for assigned assets. Review and validate inventory accuracy and perform regular asset reviews.
Line Managers	Initiate asset allocation and transfer requests for team members. Ensure assets are returned or reassigned during role transitions or terminations.
HR Department	Coordinates with IT and Line Managers during onboarding and offboarding to ensure proper asset allocation and return.
Employees and Users	Responsible for the secure use, storage, and return of assigned assets. Must comply with all relevant policies related to asset handling and protection.

5. ASSET INVENTORY MANAGEMENT

1. Asset Identification and Registration

- All organizational assets—physical, logical, and supporting—must be uniquely identified and recorded in the centralized Asset Inventory Register managed by the IT Operations Team.
- Each entry must include asset type, description, make/model, serial number (if applicable), assigned owner, classification level, location, allocation status, and lifecycle status.

2. Asset Categories

Assets shall be classified into the following categories for inventory purposes:

- **Hardware Assets**: laptops, desktops, servers, mobile devices, storage devices, networking equipment.
- **Software Assets**: licensed applications, system software, internally developed tools.
- **Information Assets**: databases, files, reports, documentation, intellectual property.
- **Supporting Assets**: ID cards, security tokens, removable media, digital certificates, cloud resources.

3. Ownership and Accountability

- Each asset must have a designated **Asset Owner** responsible for classification, usage guidelines, and periodic review.
- **Asset Custodians** may be assigned to manage the operational use of the asset, ensuring it is handled in accordance with defined controls.

4. Inventory Maintenance

- The Asset Inventory Register must be reviewed and updated on a quarterly basis to ensure accuracy and completeness.
- Changes such as transfers, disposals, or declassifications must be reflected in the inventory within 5 business days of execution.
- All updates must include timestamps and author identification to maintain traceability.

5. Asset Tagging

- All physical assets must be tagged with a unique asset ID and barcode or RFID label to enable efficient tracking.
- Digital assets (e.g., data, files, licenses) must be logged with system-level identifiers and linked to relevant business functions and owners.

6. Critical Asset Identification

- Assets deemed business-critical or security-sensitive must be marked accordingly and monitored with increased frequency.
- The Information Security Team shall maintain a list of critical assets requiring additional oversight.

6. ASSET CLASSIFICATION GUIDELINES

1. Purpose of Classification

Asset classification ensures that each asset is protected in accordance with its sensitivity, criticality, and value to the organization. The classification determines the handling, storage, access, and disposal requirements of the asset.

2. Classification Levels

All assets must be categorized into one of the following sensitivity levels:

- **Public**: Assets intended for public disclosure with no adverse impact if exposed.
- **Internal**: Assets restricted to internal personnel and not intended for external sharing.
- **Confidential**: Sensitive business or operational information requiring protection from unauthorized access.
- **Restricted**: Highly sensitive or regulated information, where unauthorized disclosure could cause significant legal, reputational, or financial harm.

Classification Level	Definition	Examples	Handling Requirements
Public	Information approved for external release with no risk if disclosed.	Published marketing materials, website content, job postings.	No restrictions; can be shared freely.
Internal	Information meant only for internal organizational use; low risk if disclosed.	Internal emails, process documentation, org charts.	Share only within the organization; store on approved systems; avoid public platforms.
Confidential	Sensitive information requiring protection from unauthorized access.	Employee records, internal financials, project plans, PII.	Access controlled on a need-to-know basis; encrypt at rest and in transit; secure storage.

Classification Level	Definition	Examples	Handling Requirements
Restricted	Highly sensitive or regulated data where unauthorized access poses serious risk.	Trade secrets, customer data, health records, credentials, encryption keys.	Strict access controls; encryption mandatory; storage only on secured/monitored systems.

3. Classification Criteria

Classification shall be determined based on factors including, but not limited to:

- Legal or regulatory obligations (e.g., PII, PHI, PCI-DSS)
- Business criticality or operational dependency
- Financial impact of unauthorized access, modification, or loss
- Risk to reputation or compliance in the event of a breach

4. Responsibilities for Classification

- The **Asset Owner** is responsible for determining the appropriate classification level at the time of asset creation or acquisition.
- The **Information Security Team** may review and advise on classification for high-risk or regulated assets.

5. Review and Reclassification

- Asset classifications must be reviewed at least annually or when there is a change in business usage, risk profile, or ownership.
- Reclassification (including upgrades or downgrades) must follow the formal approval and documentation process outlined in Section 8.

6. Documentation Requirements

- Classification levels must be recorded in the Asset Inventory Register.
- Associated handling and security controls must be documented and communicated to all relevant custodians and users.

7. ASSET VALUATION GUIDELINES

1. Purpose of Valuation

Asset valuation is performed to determine the criticality of an asset based on its importance to the **Confidentiality**, **Integrity**, and **Availability** (CIA) of [ORG

NAME]'s information and services. This valuation supports risk management, control prioritization, and impact analysis in case of asset compromise or loss.

2. Valuation Criteria

The valuation of an asset shall be based on the potential impact of its loss, disclosure, or unavailability. The following factors must be considered:

- **Confidentiality**: Sensitivity of the data or process the asset supports, and consequences of unauthorized disclosure.
- **Integrity**: Impact of unauthorized modification or corruption of the asset's information or function.
- **Availability**: Importance of the asset to maintaining operational continuity and service delivery.

Additional impact dimensions include:

- **Number of Assets Affected**: Extent to which a single incident could impact multiple assets or systems.
- **Number of Customers Affected**: Estimated scale of user or client disruption in the event of a failure or breach.
- **Financial Impact**: Direct and indirect cost implications, including loss of revenue, recovery costs, and fines.
- **Legal and Regulatory Impact**: Exposure to non-compliance, sanctions, or contractual penalties.
- **Reputational Damage**: Potential erosion of trust, media exposure, and stakeholder dissatisfaction.

Impact Level	# of Assets Affected	# of Customers Affected	Financial Impact	Legal & Regulatory Impact	Reputational Damage
Low	Single, standalone asset	None or minimal	<$1,000	No legal or regulatory exposure	No impact on brand or perception
Medium	Affects a small group or limited interdependencies	Dozens to hundreds	$1,000 – $50,000	Contractual exposure or minor regulatory implications	Internal concerns or limited stakeholder dissatisfaction
High	Large-scale or interconnected systems	Hundreds to thousands	>$50,000 or recurring losses	Violation of major laws/regulations; risk of penalties	Public/media backlash, loss of customer or stakeholder trust

3. Valuation Categories

Each asset shall be categorized into one of the following impact tiers:

- **High**: Critical asset; loss or compromise would result in severe impact across multiple criteria.
- **Medium**: Significant asset; loss would result in moderate impact, typically limited to one department or function.
- **Low**: Non-critical asset; minimal business impact if compromised.

4. Valuation Process

- Asset Owners, with support from the Information Security Team, shall assess the asset's CIA impact and assign a valuation category.
- Valuation must be recorded in the Asset Inventory Register and reviewed during asset lifecycle milestones (e.g., acquisition, reallocation, decommissioning).

5. Review and Updates

- Asset valuations must be reviewed annually or upon any material change in asset function, data sensitivity, or business environment.
- Any revaluation must be approved and updated in the Asset Inventory Register, along with a documented justification.

8. ASSET DECLASSIFICATION AND DOWNGRADING

1. Purpose

Asset declassification and downgrading ensure that classification levels remain accurate and reflect the current business, legal, and risk environment. Assets should not retain higher classifications than necessary, as this may lead to unnecessary control overhead or resource allocation.

2. Triggers for Reclassification

An asset may be considered for declassification or downgrading under the following conditions:

- The asset is no longer in active use or has reached end-of-life.
- The asset has been archived or replaced by a newer system or dataset.
- The sensitivity or business criticality of the asset has reduced.
- A formal risk assessment determines that the existing classification is no longer appropriate.

3. Review and Approval Process

- Requests for reclassification must be formally initiated by the **Asset Owner** using the Asset Classification Review Form.
- A reclassification risk assessment must be performed by the **Information Security Team**, especially for assets originally marked as "Restricted" or "Confidential."
- Final approval must be obtained from the **CISO** for all downgrades involving regulated, legal, or critical systems/data.

4. Documentation and Audit Trail

- All reclassification decisions must be documented with:
  - Justification for change
  - Approval workflow
  - Updated classification label
  - Date of change and change owner
- Changes must be reflected in the Asset Inventory Register within 5 business days.

5. Controls During Transition

- Until reclassification is approved, the asset must continue to be protected according to its original classification level.
- If declassification results in relaxed controls, compensating safeguards must be reviewed to ensure no residual risk is introduced.

9. ASSET LABELLING

1. Purpose

Asset labelling ensures that classification levels, ownership, and tracking information are visibly or logically associated with the asset, enabling appropriate handling, access, and control measures.

2. Labelling Requirements

- All physical and logical assets must be labelled in accordance with their classification level and organizational labelling standards.
- Labels must be clear, durable, and securely affixed where applicable, without exposing sensitive information to unauthorized individuals.

3. Physical Asset Labelling

- Hardware assets (e.g., laptops, servers, mobile devices) must be tagged with:

- Unique asset ID/barcode or RFID
- Owner (individual or department)
- Classification level (e.g., Confidential, Restricted) if required

- Labels should avoid including sensitive data (e.g., user credentials, encryption keys).

4. Logical Asset Labelling

- Digital files, folders, databases, and other logical assets must be labelled through:
  - Metadata tags (e.g., classification fields in document properties)
  - Watermarks for sensitive documents (e.g., "CONFIDENTIAL" headers/footers)
  - File naming conventions aligned with classification standards

5. Classification-Based Labelling Guidelines

Classification	Labelling Guidance
Public	No labelling required unless needed for version control or organizational identification.
Internal	Optional labelling; internal-only access tags recommended.
Confidential	Must be clearly marked on physical and digital assets (e.g., "Confidential - Internal Use").
Restricted	Mandatory labelling with bold headers/watermarks and secure asset ID tracking.

6. Responsibilities

- The **IT Operations Team** is responsible for physical labelling of assets during allocation.
- **Asset Owners** are responsible for ensuring appropriate labelling of digital assets.
- **Information Security Team** must periodically verify adherence to labelling protocols during audits.

7. Tampering or Removal of Labels

- Unauthorized removal, modification, or concealment of asset labels is strictly prohibited.
- Any damage to labels must be reported to the IT Operations Team for immediate replacement.

10. 10. ASSET ALLOCATION

1. Purpose

Asset allocation ensures that organizational assets are assigned to individuals, departments, or third parties in a controlled, traceable, and authorized manner. This helps maintain accountability and proper usage in alignment with business needs and security requirements.

2. Allocation Eligibility

- Only authorized personnel with a valid business need may be allocated organizational assets.
- Allocation must be based on job function, role responsibilities, and classification of the asset.

3. Allocation Process

- Asset allocation must be formally requested by the user's **Line Manager** via the designated asset request workflow or IT ticketing system.
- Each request must include:
  - Justification for the asset
  - Type of asset required
  - Intended duration of use (if temporary)
- Requests must be reviewed and approved by the **IT Operations Team** and, for high-risk assets, by the **Information Security Team** or **Asset Owner**.

4. Acknowledgment and Assignment

- Upon approval, the recipient must sign an **Asset Allocation Acknowledgment Form** confirming:
  - Receipt of the asset
  - Understanding of responsibilities
  - Compliance with Acceptable Use and Asset Management policies
- The asset's status and custodian information must be updated in the **Asset Inventory Register**.

5. Temporary Allocation

- Temporary allocations (e.g., short-term project use, testing) must include:
  - Start and end dates
  - Conditions for return
  - Expiry-driven tracking
- Temporary assets must be clearly labeled and flagged in the inventory for follow-up.

6. Special Cases

- High-risk or sensitive assets (e.g., encrypted USBs, privileged access laptops) may require enhanced controls such as additional approvals, usage monitoring, or restricted functionality.
- Asset allocation to third parties must be covered by contractual agreements, including terms for asset protection, usage limitations, and return obligations.

7. Responsibilities of Asset Holders

- Maintain the asset in good working condition and report any loss, damage, or misuse immediately.
- Use the asset strictly for authorized business purposes.
- Not transfer the asset to another individual without formal reallocation approval.

11. ASSET HANDLING AND PROTECTION

1. Purpose

Proper handling and protection of assets ensure that their confidentiality, integrity, and availability are preserved throughout their lifecycle. All users are responsible for safeguarding the assets under their custody against unauthorized access, loss, damage, or misuse.

2. General Handling Guidelines

- Assets must be used only for approved organizational activities and in accordance with their classification level.
- Physical and logical access to assets must be limited to authorized individuals.
- Unauthorized modifications, installations, or alterations to assets are strictly prohibited.

3. Physical Protection

- Hardware assets must be stored in secure, access-controlled environments.

- Portable devices (e.g., laptops, mobile phones) must be secured with locks, tracking features, or encryption when not in use or when transported.
- Confidential and restricted assets must not be left unattended in unsecured or public areas.

4. Environmental Controls

- Assets housed in data centers or critical infrastructure zones must be protected with climate control, fire suppression, power backup, and physical security systems.
- Users must not expose IT assets to conditions likely to cause environmental damage (e.g., moisture, heat, magnetic interference).

5. Logical Protection

- Information assets must be stored on approved, secure platforms with access controls, encryption (where applicable), and regular backups.
- Access to systems, files, or databases must follow the principle of least privilege and must be granted based on role-based access controls (RBAC).

6. Sensitive Data Handling

- Data classified as Confidential or Restricted must be encrypted during transmission and stored only on secured systems.
- Physical printouts must be stored in locked cabinets and securely destroyed when no longer needed.

7. Monitoring and Alerts

- All high-risk asset usage must be logged and subject to monitoring by the Information Security Team.
- Anomalies or policy violations must trigger alerts and be reviewed as potential security **incidents.**

8. User Responsibilities

- Report any suspected compromise, theft, or misuse of assets immediately to the IT or Security Team.
- Follow clear desk and clear screen practices, especially in shared or public environments.
- Refrain from leaving authentication tokens, passwords, or sensitive material exposed or accessible.

12. ASSET MAINTENANCE

1. Purpose

Routine and secure maintenance of assets ensures operational reliability, performance consistency, and prolonged asset lifecycle while minimizing security vulnerabilities and unplanned outages.

2. Types of Maintenance

- **Preventive Maintenance**: Scheduled upkeep activities to avoid asset failure (e.g., firmware updates, hardware servicing).
- **Corrective Maintenance**: Unscheduled repair or support activities in response to identified faults or incidents.

3. Maintenance Responsibilities

- The **IT Operations Team** is responsible for planning and executing maintenance of hardware and system software assets.
- Asset Owners must coordinate with IT to schedule maintenance without disrupting business operations.
- For sensitive assets, the **Information Security Team** must be notified before any major maintenance is performed.

4. Secure Maintenance Requirements

- Maintenance must only be conducted by authorized personnel (internal or approved third parties).
- All maintenance activities must be logged, including:
  - Date and time of maintenance
  - Asset ID
  - Description of activity performed
  - Personnel involved
- Systems handling Confidential or Restricted data must not be taken off-site for repair unless approved by the CISO.

5. Third-Party Involvement

- All third-party vendors performing maintenance must:
  - Sign confidentiality and non-disclosure agreements
  - Be supervised if accessing secure environments or sensitive data

- Adhere to organizational security and access control standards

6. Post-Maintenance Validation

- After maintenance, the asset must be validated for proper functioning and checked for:
  - Re-application of security configurations and controls
  - Restoration of patches, access rights, and encryption (if applicable)
- Any deviation or risk observed must be reported to the Information Security Team for follow-up.

7. Recordkeeping and Audit

- Maintenance records must be retained for a minimum of 12 months or as per the Data Retention Policy.
- These records are subject to internal and external audits for compliance verification.

13. INWARD AND OUTWARD MOVEMENT OF ASSETS

1. Purpose

To ensure that any physical movement of organizational assets—whether incoming or outgoing—is authorized, documented, and traceable. This reduces the risk of loss, theft, or unauthorized removal of company property.

2. Inward Movement (New or Returning Assets)

- All incoming assets (e.g., new purchases, returns from service, or transfers from other offices) must be logged in the **Asset Inventory Register** upon receipt.
- The **IT Operations Team** must verify asset condition, match against purchase records or return documentation, and update:
  - Serial numbers, asset IDs, owner, and classification
  - Status as "Received" and location assigned
- Returned assets must undergo inspection, data sanitization (if previously allocated), and reconfiguration before being reissued or stored.

3. Outward Movement (Temporary or Permanent)

- Any asset leaving [ORG NAME] premises for offsite work, vendor servicing, or transfers must be authorized and documented using the **Asset Movement Authorization Form** or asset gate pass system.
- Mandatory fields include:

- Asset ID and type
- Purpose of movement
- Person responsible
- Expected return date (for temporary movements)
- Approval from Line Manager and IT Operations

4. Gate Pass and Tracking

- Physical gate passes (paper or digital) must be issued by IT or Facilities for assets leaving the premises.
- Security personnel must verify gate pass details before allowing removal.
- Any discrepancy must be reported to the IT Operations Team immediately.

5. Temporary Movement

- Assets moved for events, remote work, or field activities must be returned within the approved timeline.
- Delays or incidents (e.g., damage, loss) must be reported immediately and **documented.**

6. Permanent Movement or Transfer Between Locations

- Asset transfers between branches, business units, or to other company-owned premises must:
  - Be approved by both sending and receiving unit heads
  - Include updated records in the Asset Inventory Register
  - Be validated upon receipt by the receiving team

7. Loss or Non-Return

- Any asset not returned by the approved return date or found missing must be treated as a potential **security incident**.
- The user may be held accountable for replacement or recovery costs, subject to HR and IT policies.

14. ASSET TRANSFER AND REALLOCATION

1. Purpose

Asset transfer and reallocation ensure that organizational assets are reassigned in a controlled and auditable manner when roles change, departments reorganize, or equipment is shared between users or locations.

2. Transfer Scenarios

Asset transfers may include:

- **User-to-user**: e.g., replacement of staff, role change, or temporary assignment.
- **Department-to-department**: e.g., project transitions, organizational restructuring.
- **Location-to-location**: e.g., movement of assets across branch offices or data centres.

3. Transfer Initiation and Approval

- All transfers must be formally requested via the asset transfer form or IT ticketing system.
- The request must include:
  - Asset ID and current custodian
  - Reason for transfer
  - New owner or location
  - Transfer date
- Approvals must be obtained from:
  - The current Asset Owner or Line Manager
  - Receiving department's Line Manager or designated owner
  - IT Operations Team (for validation and record updates)

4. Pre-Transfer Checks

- The IT Operations Team must verify:
  - Physical condition of the asset
  - Removal of any user-specific data or credentials
  - Whether a reset or reconfiguration is required before handover

5. Reallocation and Inventory Update

- Upon successful handover, the Asset Inventory Register must be updated with:
  - New owner/custodian information
  - Updated location (if applicable)
  - Date and confirmation of reallocation
- A new **Asset Allocation Acknowledgment Form** must be signed by the receiving party.

6. Security Considerations

- For assets classified as **Confidential** or **Restricted**, all prior user data must be securely wiped or archived before reallocation.
- Access controls, encryption, and software licenses must be reviewed and updated for the new user.

7. Recordkeeping

- All transfer and reallocation activities must be documented and retained for audit purposes in accordance with the Data Retention Policy.
- Transfer logs must be made available during internal reviews or compliance audits.

15. ACCEPTABLE USE OF ASSETS

1. Purpose

To define clear expectations and permissible use of organizational assets to prevent misuse, ensure data security, and maintain operational efficiency.

2. General Usage Principles

- All assets must be used strictly for authorized business purposes.
- Users must follow applicable organizational policies including the **Acceptable Use Policy**, **Information Security Policy**, and this **Asset Management Policy**.
- Users are accountable for the assets issued to them and must not share, modify, or transfer them without prior approval.

3. Authorized Use Only

- Use of any asset (hardware, software, or data) must be aligned with the user's role and approved responsibilities.
- Unauthorized installation of software, connecting personal devices to enterprise networks, or using company resources for personal financial gain is prohibited.

4. Security Practices

- Users must not bypass technical controls (e.g., antivirus, firewalls, encryption).
- Systems must be locked or logged off when unattended.
- Passwords, tokens, and authentication mechanisms must be kept secure and not shared.

5. Data Handling

- Confidential or Restricted data must be stored, processed, and transmitted using approved secure systems.
- Use of removable media must comply with the organization's removable media policy and require prior IT approval.

6. Personal Use Restrictions

- Limited personal use may be permitted (e.g., personal browsing or email) as long as it:
  - Does not interfere with work duties,
  - Does not involve prohibited activities (e.g., gambling, harassment),
  - Does not violate any organizational policies or laws.

7. Monitoring and Logging

- Use of organizational assets is subject to monitoring in accordance with the **Privacy and Monitoring Policy**.
- Any evidence of misuse or policy violations may result in disciplinary actions.

8. Reporting Misuse

- Users must report any suspected or actual misuse of assets to their Line Manager or the Information Security Team immediately.

16. ASSET RETURN AND DISPOSAL

1. Purpose

To ensure that all organizational assets are securely returned at the end of their use and disposed of in a manner that protects sensitive information, complies with legal and environmental requirements, and maintains inventory integrity.

2. Asset Return Requirements

- All assets must be returned to the **IT Operations Team** upon:
  - Termination or resignation of the user
  - Role change or internal transfer
  - Expiry of temporary allocation or project completion
- Line Managers and HR must notify IT during offboarding to trigger asset return procedures.
- Users must return:
  - All hardware (e.g., laptops, mobile devices, tokens)
  - All physical documentation

- Any assigned accessories (e.g., chargers, docking stations, security keys)

3. Asset Return Process

- Returned assets must be inspected for physical damage and validated against the Asset Inventory Register.
- Users must sign an **Asset Return Acknowledgment Form**, and the asset's return must be recorded in the inventory system.
- Any missing, lost, or damaged assets must be reported and investigated as a **security incident**.

4. Data Sanitization Prior to Disposal or Reallocation

- All storage media (e.g., hard drives, SSDs, USBs) must be securely wiped using approved tools before reuse, transfer, or disposal.
- Assets containing **Restricted** or **Confidential** data must follow data destruction procedures as outlined by the Information Security Team.
- Certificates of data destruction must be retained for audit purposes where applicable.

5. Disposal Procedures

- Disposal of IT equipment and media must:
  - Be handled by authorized personnel or certified vendors
  - Comply with the organization's **Data Retention Policy**, **Environmental Policy**, and applicable e-waste laws
  - Be logged with details such as asset ID, disposal method, disposal vendor, and date
- The **IT Operations Team** is responsible for ensuring compliance and updating the Asset Inventory Register.

6. Asset Lifecycle Status

- Upon disposal, the asset's status in the inventory must be updated to "Disposed" with relevant metadata including:
  - Date of disposal
  - Method used (e.g., shredding, degaussing, recycling)
  - Approval reference or certificate ID (if applicable)

7. Audit and Verification

- Disposal records must be retained for a minimum of 24 months or as required by regulation.

- The Information Security Team will review disposal activities during regular asset lifecycle audits.

17. ENFORCEMENT

1. **Policy Compliance**

   - All employees, contractors, vendors, and third-party users with access to [ORG NAME] assets are required to adhere strictly to this Asset Management Policy.
   - Any misuse, negligence, or unauthorized activity involving organizational assets will be considered a violation and addressed accordingly.

2. **Examples of Violations**

   Violations include, but are not limited to:

   - Failure to return organizational assets upon offboarding or transfer
   - Unauthorized transfer, reallocation, or modification of assets
   - Use of assets for personal financial gain or prohibited activities
   - Negligent handling resulting in loss, damage, or data breach
   - Disposal of assets without following sanitization and decommissioning procedures

3. **Disciplinary Actions**

   Based on the severity and intent of the violation, disciplinary actions may include:

   - Verbal or written warning
   - Suspension of system or asset access rights
   - Formal HR disciplinary action
   - Financial recovery of asset replacement costs
   - Termination of employment or contract
   - Legal action in accordance with applicable laws

4. **Reporting of Violations**

   - All suspected or actual violations must be reported immediately to the **Information Security Team** or via the service desk ticketing system.
   - The incident shall be documented and managed in accordance with the **Incident** Management **Policy**.

5. **Corrective and Preventive Actions (CAPA)**

- Upon resolution of an incident, appropriate CAPA measures shall be implemented, which may include:
  - Process or policy updates
  - Additional user training
  - Deployment of technical controls
  - Enhanced monitoring or escalation thresholds

6. **Retention of Enforcement Records**

- All enforcement records, including investigation details, communications, and resolutions, must be retained securely for a minimum of 24 months or longer if required by law or audit regulations.

18. POLICY EXCEPTIONS

1. Request for Exception

- Any deviation from the defined standards in this Asset Management Policy must be requested formally using the IT Policy Exception Request Form.
- Requests must contain:
  - Business justification and scope of the exception
  - Duration for which the exception is needed
  - Risk assessment and impact analysis
  - Any proposed compensating controls

2. Approval Workflow

- All exception requests must follow a structured multi-level approval process:

Level	Approver
Level 1	Department Head / Business Unit Owner
Level 2	Application/System Owner
Level 3	Information Security Officer (ISO)
Level 4	Chief Information Security Officer (CISO)

- The CISO holds final authority to approve, deny, or revoke an exception.

3. Documentation and Register Maintenance

- Approved exceptions must be recorded in the Exception Register maintained by the Security & Compliance Office.
- Each entry must include requester details, approval chain, expiry date, and applicable controls.

4. Time Bound Validity and Review

- Exceptions must be time-bound and reviewed periodically.
- Default maximum validity shall not exceed 90 days unless formally extended and reapproved.
- Active exceptions shall be reviewed monthly to ensure continued relevance and risk containment.

5. Compensating Controls

- If an exception introduces additional risk, mitigating or compensating controls must be enforced. Examples include:
  - Enhanced logging and monitoring
  - Restricting access scope or duration
  - Additional user validation or supervision

6. Revocation and Audit

- The CISO reserves the right to revoke an exception if:
  - The associated risk becomes unacceptable
  - The business justification no longer applies
  - Evidence of misuse or policy breach is found
- All exceptions shall be subject to review during internal and external audits.
- Non-compliance with the approved terms of the exception may lead to enforcement actions as defined in Section 17.

19. ESCALATION MATRIX

In case of access management-related issues, violations, or delays in provisioning/de-provisioning, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Escalation Level	Role/Designation	Responsibility	Contact Mode
Level 1	Reporting Manager / Team Lead	First-level resolution and access validation	Email / Ticketing Tool
Level 2	System/Application Owner	Review of access alignment with business roles	Email / Phone
Level 3	IT Operations Manager	Resolution of system-level or technical delays	Internal escalation call
Level 4	Information Security Officer (ISO)	Security assurance and compliance validation	Email / Escalation Tool
Level 5	Chief Information Security Officer	Final authority on policy enforcement and risk mitigation	Direct escalation via email / formal report

- Escalations must be documented through the ITSM tool or equivalent service desk system.
- Each escalation must include clear description of the issue, impacted users/systems, time of initial request, and business impact.
- SLAs for resolution based on priority level shall be defined and tracked by the IT Service Management function

DID YOU FIND THIS DOCUMENT USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

WWW.MINISTRYOFSECURITY.CO