Asset Management Policy

July 2nd, 2024 version

Table of Contents

1. Purpose and Scope

Purpose

The purpose of this Asset Management Policy is to establish a comprehensive framework for the management, protection, and utilization of the organization's information assets. This policy aims to ensure that all assets, including hardware, software, data, and intellectual property, are identified, classified, used, maintained, and disposed of in a manner that preserves their confidentiality, integrity, and availability. By implementing this policy, our organization seeks to:

- Protect Information Assets: Safeguard all assets from unauthorized access, disclosure, alteration, and destruction.
- Ensure Regulatory Compliance: Adhere to relevant legal, regulatory, and contractual requirements concerning information security and asset management.
- Optimize Operational Efficiency: Enhance resource utilization through efficient asset management practices, reducing redundancies and ensuring effective allocation of assets.
- Mitigate Risks: Identify, assess, and manage risks associated with information assets to minimize potential operational, reputational, and financial impacts.
- Enable Effective Incident Response: Establish protocols for quick and effective responses to security incidents involving information assets, minimizing damage and ensuring rapid recovery.
- Promote Accountability: Clearly define roles and responsibilities for asset management, ensuring that all employees understand their obligations and the importance of protecting information assets.
- Support Strategic Objectives: Align asset management practices with the organization's broader strategic objectives, ensuring that information assets contribute to overall mission and goals.

Scope

The scope of this Asset Management Policy encompasses all aspects of the organization's operations that involve information assets. This includes all departments, business units, and personnel, as well as external parties such as contractors, consultants, and third-party service providers who have access to or manage the organization's information assets.

Information Assets:

- Hardware:
    - Portable PCs used by developers
    - Fixed PCs used by developers
    - Portable PCs used by sales, marketing, and support functions
    - Fixed PCs used by sales, marketing, and support functions
    - Servers in datacenters
    - Servers at OVH (supplier)
- Software:
    - Applications, operating systems, utilities, and middleware used within the organization, including those developed in-house and acquired from external vendors.

- Data:
    - Source code and protected intellectual property stored on encrypted drives or folders on PCs used by developers.
    - Client's data, which must always remain on servers located in datacenters or at OVH and never leave these locations.
    - Commercial and marketing information stored on PCs used by sales, marketing, and support functions.
    - Sensitive personal information from clients and employees stored on PCs used by sales, marketing, and support functions.
- Intellectual Property:
    - Software code and hardware and electronics plans stored on PCs used by developers, which constitute the majority of the company's intellectual property.

Lifecycle Phases

- Acquisition: Procuring or developing new information assets, including defining requirements, selecting vendors, and negotiating contracts.
- Deployment: Installing, configuring, and integrating information assets into the organization's environment.
- Maintenance: Ongoing management, monitoring, and support of information assets to ensure optimal performance and security.
- Utilization: Day-to-day use of information assets by authorized personnel.
- Disposal: Secure decommissioning and disposal of information assets that are no longer needed, ensuring all sensitive information is permanently removed or destroyed.

Asset Management Activities

- Inventory Management: Maintaining a comprehensive and up-to-date inventory of all information assets, including detailed records of asset attributes, ownership, location, and status.
- Asset Classification: Categorizing information assets based on sensitivity, criticality, and value to the organization, and applying appropriate security controls.
- Access Control: Implementing and managing access controls to ensure only authorized individuals have access to information assets, based on the principle of least privilege and need-to-know.
- Risk Management: Identifying and assessing risks associated with information assets, and implementing measures to mitigate those risks.
- Security Measures: Applying technical and administrative controls to protect information assets from threats.
- Incident Response: Establishing procedures for detecting, reporting, and responding to security incidents involving information assets, and conducting post-incident analysis and remediation.
- Compliance and Audit: Ensuring adherence to internal policies, industry standards, and legal requirements through regular audits and assessments.

Implementation and Enforcement

The successful implementation of this Asset Management Policy requires the cooperation and commitment of all personnel within the organization. To ensure effective enforcement, the following measures will be undertaken:

1. Communication: The policy will be communicated to all employees and relevant external parties through training sessions, internal communications, and accessible documentation.
2. Training and Awareness: Regular training programs will be conducted to educate employees on the importance of asset management, their responsibilities, and the procedures outlined in the policy.
3. Monitoring and Reporting: Continuous monitoring of information assets will be carried out to detect any unauthorized activities or security incidents. Employees are encouraged to report any suspicious activities or potential security breaches.
4. Audit and Review: Regular audits and reviews of the asset management practices will be conducted to ensure compliance with the policy and identify areas for improvement. Audit findings will be reported to senior management and corrective actions will be taken as necessary.
5. Policy Updates: The Asset Management Policy will be reviewed and updated periodically to reflect changes in the organizational environment, technological advancements, and evolving security threats. Any updates to the policy will be communicated to all relevant parties.

2. Roles and Responsibilities

Effective asset management is a collective effort that involves various roles and responsibilities across the organization. This section defines the specific duties and expectations for each role involved in the management and protection of the organization's information assets.

Chief Technology Officer (CTO)

The CTO is responsible for overseeing the development team and the management of all servers, both in datacenters and at OVH, ensuring the proper management and protection of all related assets. Specific responsibilities include:

- Asset Protection: Ensure that all PCs used by developers are configured to store source code and protected intellectual property on encrypted drives or folders.
- Server Management: Oversee the management and security of servers in datacenters and at OVH, ensuring they are properly configured, maintained, and protected against unauthorized access.
- Policy Enforcement: Enforce compliance with asset management policies among the development team and server administrators, ensuring adherence to procedures for handling, storing, and accessing sensitive information.
- Resource Allocation: Allocate resources and tools necessary for secure development and server management practices, including secure coding tools, encryption software, and access control mechanisms.
- Training and Awareness: Provide training for developers and server administrators on the importance of asset protection, secure coding practices, and the specific requirements of this policy.
- Incident Response: Collaborate with the CISO and IT department to respond to security incidents involving development assets and servers, ensuring swift and effective remediation.

Chief Operating Officer (COO)

The COO is responsible for managing the sales, marketing, and support functions, ensuring that PCs used in these functions are properly managed and secured. Specific responsibilities include:

- Asset Utilization: Ensure that PCs used by sales, marketing, and support teams store only commercial, marketing, and sensitive personal information as appropriate, avoiding unauthorized storage of development code or client data.
- Policy Compliance: Enforce compliance with asset management policies within the sales, marketing, and support functions, ensuring that all personnel adhere to established procedures.
- Data Protection: Implement measures to protect sensitive personal information stored on these PCs, including encryption, access controls, and regular data audits.
- Training and Awareness: Provide training and awareness programs for sales, marketing, and support staff on the importance of asset management and data protection.
- Incident Reporting: Ensure that any security incidents involving assets in these functions are promptly reported to the CISO and IT department for investigation and resolution.

Chief Information Security Officer (CISO)

The CISO plays a critical role in overseeing the overall security of information assets across the organization. Specific responsibilities include:

- Risk Management: Conduct regular risk assessments to identify potential threats to information assets and implement appropriate mitigation strategies.
- Security Policies: Develop, maintain, and update security policies and procedures related to asset management, ensuring they are aligned with industry standards and regulatory requirements.
- Incident Response: Lead the incident response team in detecting, investigating, and responding to security incidents involving information assets. Ensure that incidents are properly documented and post-incident analysis is conducted.
- Compliance Monitoring: Monitor compliance with asset management and security policies through regular audits and assessments. Report findings to senior management and recommend corrective actions.
- Security Training: Oversee the development and delivery of security training programs for all employees, ensuring they understand their roles in protecting information assets.

IT Department

The IT Department is responsible for the technical management of information assets, including procurement, deployment, maintenance, and disposal. Specific responsibilities include:

1. Asset Inventory: Maintain a comprehensive and up-to-date inventory of all information assets, including hardware, software, and data. Ensure detailed records of asset attributes, ownership, location, and status. This can be done using Excel documents.
2. Technical Controls: Implement and manage technical controls to protect information assets, including encryption, access controls, patch management, and vulnerability assessments.
3. Deployment and Maintenance: Ensure the secure deployment and maintenance of information assets, including the installation of security updates and patches.
4. Data Backup and Recovery: Implement robust data backup and recovery procedures to protect against data loss and ensure business continuity.
5. Secure Disposal: Ensure the secure disposal of information assets that are no longer needed, including the permanent removal or destruction of sensitive information.

Asset Owners

Asset owners are individuals or departments assigned ownership of specific information assets. They are responsible for the proper management and protection of their assigned assets. Specific responsibilities include:

1. Asset Oversight: Ensure that information assets under their control are used, maintained, and protected according to the asset management policy.
2. Access Control: Manage access to assigned assets, ensuring that only authorized personnel have access based on the principle of least privilege and need-to-know.
3. Regular Reviews: Conduct regular reviews of assigned assets to ensure they are properly documented, classified, and protected.

4. Incident Reporting: Report any security incidents or potential vulnerabilities involving their assigned assets to the CISO and IT department for investigation.

All Employees

All employees have a role to play in the management and protection of information assets. Specific responsibilities include:

1. Policy Adherence: Adhere to the asset management policy and related procedures, ensuring that information assets are used and protected according to established guidelines.
2. Security Awareness: Participate in security training and awareness programs to understand the importance of asset protection and their role in maintaining security.
3. Incident Reporting: Promptly report any security incidents, suspicious activities, or potential vulnerabilities to the appropriate authorities, including the CISO and IT department.

External Parties

External parties, including contractors, consultants, and third-party service providers, may have access to the organization’s information assets and are required to comply with the asset management policy. Specific responsibilities include:

1. Compliance: Adhere to the organization's asset management and security requirements as specified in contracts and agreements.
2. Access Control: Ensure that access to the organization's information assets is restricted to authorized personnel only.
3. Security Measures: Implement appropriate security measures to protect the information assets they manage or access, in line with the organization's policies.
4. Incident Reporting: Report any security incidents or potential vulnerabilities involving the organization’s information assets to the designated contact within the organization.

Senior Management

Senior management is responsible for providing strategic direction, approving the asset management policy, and ensuring the necessary resources and support for its implementation. Specific responsibilities include:

1. Policy Approval: Review and approve the asset management policy and any subsequent updates.
2. Resource Allocation: Allocate sufficient resources to support the implementation and maintenance of the asset management policy.
3. Leadership Support: Demonstrate commitment to asset management and information security by promoting a culture of security and accountability within the organization.
4. Oversight: Monitor the effectiveness of the asset management policy and practices, and provide guidance and support for continuous improvement.

3. Asset Lifecycle Management

Asset Lifecycle Management (ALM) is essential for maximizing the value of an organization's assets from acquisition to disposal. Our approach ensures efficient utilization, proper maintenance, and responsible disposal while minimizing costs and risks.

Acquisition

The acquisition phase begins with a thorough needs assessment, identifying specific requirements based on business needs, technological advancements, and user demands. Budgeting is then conducted, considering initial purchase costs, implementation expenses, and ongoing maintenance. Selection and procurement involve evaluating vendors based on cost, quality, reliability, and support services. After issuing a Request for Proposal (RFP) and reviewing responses, the organization selects the most suitable vendor and issues a purchase order. Upon delivery, each asset is tagged with a unique identifier for tracking purposes and entered into the respective Excel sheets for office PCs, developer PCs, and servers.

Deployment

Deployment involves installing and configuring assets according to organizational standards and vendor guidelines. This includes setting up hardware, installing software, and configuring network settings, followed by thorough testing. User training is provided to ensure effective operation and maintenance of the assets, involving training sessions, user manuals, and ongoing support. Comprehensive documentation is created, detailing configuration settings, installation procedures, and maintenance schedules.

Operation and Maintenance

The operation and maintenance phase ensures assets remain functional and efficient throughout their lifecycle. Regular monitoring and performance management track assets' efficiency, reliability, and usage. Preventive maintenance tasks, such as routine inspections, software updates, and hardware servicing, are scheduled regularly. Corrective maintenance is performed as needed. Security management includes implementing access controls to restrict unauthorized access and regularly updating security software and firmware.

Asset Optimization

Optimizing asset utilization involves analyzing usage data to identify underutilized or overutilized assets, allowing for informed decisions about asset allocation and improving efficiency. Cost management calculates the total cost of ownership (TCO) for each asset, considering acquisition, maintenance, operational, and disposal costs. This helps identify cost reduction opportunities, such as negotiating better maintenance contracts, using energy-efficient assets, and consolidating redundant assets.

Asset Disposal

Disposal begins with an end-of-life assessment to determine when an asset has reached the end of its useful life. Factors include performance degradation, maintenance costs, technological obsolescence, and changing business needs. Data wiping ensures all sensitive

information is securely erased before disposal, using certified tools to prevent data breaches. Components that can be recycled or repurposed are identified, and certified e-waste recycling vendors are engaged for environmentally responsible disposal. The disposal process is documented in the Excel sheets, including disposal date, method, and any associated costs or revenue.

Continuous Improvement

Continuous improvement involves collecting user feedback on asset performance and usability to identify areas for improvement. Benchmarking against industry standards ensures the organization remains competitive and efficient. Staying informed about emerging technologies, such as IoT, AI, and data analytics, is crucial for enhancing asset management capabilities. Regular upgrades to the AMS and other tools are performed to incorporate new features and improve usability and security.

Compliance and Risk Management

Ensuring compliance with relevant laws and regulations, including data protection and environmental regulations, is essential. Accurate records of asset management activities are maintained, and reports are provided to regulatory authorities as required. Risk management involves regular assessments to identify potential threats to asset security, performance, and compliance, with mitigation strategies developed and implemented. An incident response plan addresses asset-related incidents, ensuring prompt investigation and corrective actions to prevent recurrence.

Through this structured approach to ALM, our organization ensures efficient asset utilization, optimal performance, and responsible disposal, supporting overall business objectives.

4. Policies

This policy is the consequence of the previous three sections.

Hardware, Software, Applications, and Data

- All hardware, software and applications must be approved and purchased by TEEPTRAK IT.
- Installation of new hardware or software, or modifications made to existing hardware or software must follow approved TEEPTRAK procedures and change control processes.
- All purchases must follow the defined TEEPTRAK (Technology) Purchasing Standard.
- Software used by TEEPTRAK employees, contractors and/or other approved third parties working on behalf of TEEPTRAK, must be properly licensed.
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g. personally identifiable information (PII), protected health information (PHI), corporate financial data, etc.
- Two-factor authentication is required for external cloud computing applications with access to any confidential information for which TEEPTRAK has a custodial responsibility.
- Contracts with cloud computing applications providers must address data retention, destruction, data ownership and data custodian rights.
- Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
- A general inventory of information (data) must be mapped and maintained on an ongoing basis.
- All TEEPTRAK assets must be formally classified with ownership assigned.
- Maintenance and repair of organizational assets must be performed and logged in a timely manner and managed by TEEPTRAK IT Management.
- TEEPTRAK assets exceeding a set value, as determined by management, are not permitted to be removed from TEEPTRAK's physical premises without management approval.
- All TEEPTRAK physical assets exceeding a set value, as determined by management, must contain asset tags or a similar means of identifying the equipment as being owned by TEEPTRAK.
- Confidential information must be transported either by an TEEPTRAK employee or a courier approved by IT Management.
- Upon termination of employment, contract, or agreement, all TEEPTRAK assets must be returned to TEEPTRAK IT Management.

Mobile devices

- The use of a personally owned mobile devices to connect to the TEEPTRAK network is a privilege granted to employees only upon formal approval of IT Management.
- Mobile devices that access TEEPTRAK email must have a PIN or other authentication mechanism enabled.

- Confidential data should only be stored on devices that are encrypted in compliance with the TEEPTRAK Encryption Standard.
- All mobile devices should maintain up-to-date versions of all software and applications.

Media Destruction and Re-Use

- Media that may contain confidential or internal information must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
- Media reuse and destruction practices must be conducted in compliance with TEEPTRAK Data Retention & Destruction Policy.
- All decommissioned media must be stored in a secure area prior to destruction.
- Media reuse and destruction practices must be tracked and documented.
- All information must be destroyed when no longer needed, included encrypted media.

Backup

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.
- The TEEPTRAK backup and recovery process for each system must be documented and periodically reviewed according to the defined review schedule.
- The vendor(s) providing offsite backup storage for TEEPTRAK must be formally approved to handle the highest classification level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest TEEPTRAK sensitivity level of information stored.
- A process must be implemented to verify the success of the TEEPTRAK electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable in accordance with the backup standard.
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss.
- Procedures between TEEPTRAK and the offsite backup storage vendor(s) must be reviewed at least annually.
- Backups containing confidential information must be encrypted in accordance with the Encryption Standard or protected physically and properly secured from a confidentiality perspective.

Removable Media

- The use of removable media for storage of TEEPTRAK Information must be supported by a reasonable business case.
- All removable media use must be approved by TEEPTRAK IT prior to use.
- Personally owned removable media use is not permitted for storage of TEEPTRAK information.

- Users are not permitted to connect removable media from an unknown origin, without prior approval from TEEPTRAK IT.
- Confidential and internal TEEPTRAK information should not be stored on removable media without the use of encryption.
- The loss or theft of a removable media device that may have contained any TEEPTRAK information must be reported to the TEEPTRAK IT.
- The transfer of information to removable media can be monitored.

PC types and brands – Hardware specifications

Laptops must belong to one of these three models:

- Lenovo Thinkpad Carbon X1
- Lenovo Thinkpad T14(s)
- Lenovo Thinkpad P14s

Tower PCs are generally custom-made PCs using AMD processors and best price/performance hardware.

Servers are custom made using AMD processors and best price/performance hardware.

Samsung 990 PRO or Samsung PM9A3 or Western Digital SATA WD Gold are preferred disk options.

PCs should be under warranty at all time (3 years with Lenovo). After the warranty period, PCs should be disposed of without engaging the company responsibility and with no sensitive/confidential information on them (see “Media Destruction and Re-Use”).

5. Policy Review and Updates

The Asset Management Policy is a dynamic document that requires regular reviews and updates to remain effective and aligned with the organization's evolving needs. This section outlines the procedures for reviewing and updating the policy to ensure continuous improvement and compliance with current regulations and best practices.

The policy shall be reviewed annually by the Asset Manager, in collaboration with the CTO, COO, and CISO. The review process will assess the policy's effectiveness, identify areas for improvement, and incorporate feedback from relevant stakeholders. Significant changes in technology, regulatory requirements, or organizational structure may prompt more frequent reviews.

During the review, the following elements will be evaluated:

- Compliance with current laws and regulations.
- Alignment with industry standards and best practices.
- Effectiveness of existing asset management processes.
- Feedback from department heads and employees on policy implementation.
- New risks or vulnerabilities identified since the last review.
- Proposed updates will be documented and presented to senior management for approval. Once approved, the updated policy will be communicated to all employees, and necessary training will be provided to ensure compliance. Records of each review and update will be maintained to demonstrate the organization's commitment to effective asset management.

6. Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.
Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

7. Training and Awareness

Ensuring that all employees understand and adhere to the Asset Management Policy is critical for its success. This section outlines the training and awareness initiatives that will be implemented to promote compliance and foster a culture of security within the organization.

All new hires will receive comprehensive training on the Asset Management Policy as part of their onboarding process. This training will cover the importance of asset management, the types of assets covered, roles and responsibilities, and specific procedures for handling and protecting company assets. Additionally, employees will be provided with practical guidance on the use of encryption, secure storage practices, and data handling protocols.

To maintain a high level of awareness, mandatory refresher training sessions will be conducted annually for all employees. These sessions will highlight any updates to the policy, reinforce best practices, and address common issues or questions. Specialized training will be provided for developers, sales, marketing, and support functions to address their unique asset management needs and responsibilities.

Regular awareness campaigns, including emails, posters, and workshops, will be organized to keep asset management at the forefront of employees' minds. The CISO will oversee the training and awareness program, ensuring that it is effective and that all employees are equipped with the knowledge and skills to protect the organization’s assets.

8. Version History

V	Modified Date	Approved Date	Approved by	Comment
1	07/02/2023			First draft
2	08/02/2023			Change form “Destruction policy” to “Data retention & destruction policy” in 2.3
3	02/07/2024	02/07/2024	F. Coulloudon	Complete review