Walr ISMS Information Security Policy

Purpose of this policy

The purpose of the Walr Information Security Policy is to establish effective controls for computing, telecommunications, networks, and information systems. Steps must be taken to ensure the confidentiality, integrity, and availability of all information in Walr (whether generated within the business or entrusted to Walr by third parties); this means that the information must be accurate, timely, relevant, complete and protected appropriately.

Appropriate practices, procedures and technology must be implemented to protect assets that process, store, and transmit Walr information in digital, as well as non-digital formats.

This document contains policy statements that have been developed to define information protection practices critical to Walr.

The Information Security Policy shall apply to:

- All full and part-time employees, regardless of length of service, including employees on a fixed term contract
- All Walr group functions and locations
- All third parties that use Walr information and software

Information security ownership and classification

Information assets should have a designated owner. The owner decides on their sensitivity (degree of confidentiality) and criticality and classifies them according to Walr information classification standards.

The following applies:

- Information assets must have a designated owner;
- Information assets must be protected from misuse, disclosure, theft, or inappropriate modification, including information assets entrusted to Walr by third parties;
- Information must be classified on the basis of their sensitivity and degree of confidentiality;
- Criticality of information asset must be determined for purposes of Business Continuity.

The three categories used to classify the sensitivity of information assets are as follows:

Classification	Rating	Description
Public	1	Unrestricted information that can be released freely outside of Walr or made available on-demand to the general public.
Internal	2	Information appropriate for general disclosure within Walr and to authorised third parties that have a business relationship with Walr, but not to the public in general. This is the default classification for all information within Walr. Information that is assessed to be sensitive where its unauthorised disclosure could cause significant embarrassment or damage to Walr or one of its interested parties. Any release to new third parties must be covered by Walr NDA.
Confidential	3	Information that is assessed to be sensitive where its unauthorised disclosure could cause substantial damage to Walr finances or economic and commercial interests. This classification requires the information to be handled with extreme care by those entitled to a copy of it or who need to have access to it arising from their job functions. Any release to third parties must be covered by a current NDA and release must be approved by executive management.

Note: The default classification for Walr assets is internal.

Labelling and handling information

All information assets should be labelled with the appropriate classification. Where information is not labelled the following general guidelines apply. Where doubt exists, the Information Asset owner must be consulted.

Information Asset	Examples	Owner	Classification
Software Platform (Cloud)	Legacy Source Code, Platform Source Code, API Keys.	CTO	Confidential
Research Services (Europe and US)	Client Materials, PII Sample Files	COO	Confidential
Administration (Finance / HR)	Payroll Information, Legal and Regulatory Information, Training and Development records	CFO	Confidential
Global Governance / Commercial	Corporate KPIs, Revenue Information, Customer Information	CCO	Confidential
Marketing	Website Data, Industry Reporting, Brand Imaging assets	CCO	Confidential
Administration India	Employment contracts, Employee information, payroll information	COO	Confidential
Nordic Operational Data	Customer contracts, Supplier Information, Customer training information	Head of Nordics	Confidential

The default classification is the minimum classification for unlabeled information which is internal. Information may be classified higher or lower than the default classification by its label. For example, agreements may be classified Confidential (unlabeled) or Public (labelled) depending on the destination of the agreement.

All information assets should also be handled in a manner appropriate with its classification. Physical assets with a classification of Confidential and should be physically secure at all times or under the personal control of a Walr employee until the time the responsibility for this information is transferred to another party. Transferring these assets by hand is acceptable.

Information assets with a classification of Confidential or higher should not be in view of personnel not authorised to view them. In general, this requires this material to be placed out-of-sight when not in use.

Compliance enforcement

It is mandatory that all users at any level, with access to any information system within Walr, whether the user is directly employed by Walr, contracted or otherwise authorised to use Walr information assets, comply with the directives in this Information Security Policy, supporting policies, standards, guidelines and procedures for protection of information assets.

Users of information assets are reminded that:

- Nothing in the Information Security Policies overrides an article of Law
- Information held by Walr is confidential and protected, but that Walr is required to comply with the relevant Freedom of Information Acts within the jurisdictions in which the Walr business operates
- Unauthorised actions may be subject to prosecution under both country, state and local statutes and involve law enforcement officers and legal action
- All copyright and licensing requirements must be complied with
- Breach of any of the policies of the ISMS or other Walr policies may result in disciplinary action including dismissal and/or the involvement of law enforcement

Physical asset management

Asset management is about discovery, ownership, value, acceptable use, protection, and disposal of information-related assets. Assets can be tangible, like hardware, or intangible, like software, data, and knowledge. In this section, we are focused on physical assets.

The key starting point is:

- Know what we have;
- Know where it is;
- Know who owns it and who maintains it; and,
- Know how important it is to Walr.

Each of these points are expanded upon below.

Know What You Have

- Create a spreadsheet of the items:
  - List the assets for each category; and,
  - Define distinct categories or descriptions.

Know Where It Is

- Record the physical location of the asset or owner in our spreadsheet.

Know Who Owns It and Who Maintains It

- Identify and record the Owners for each of the assets. Most of the times, the individuals responsible for the security of the asset and ensuring compliance are not the same as the individuals responsible implementing security controls and day-to-day operations.

Know How Important It Is to the Business

- Review the applicable regulations, rules or company policies that require protection of information resources;
- Review Walr information classification guidelines.

All new digital equipment should be formally requested using the appropriate procedures and approved by a member of the management team prior to submission of purchase orders.

Physical inventory of assets

The Physical Asset Register is owned by Technology. Entries to the Asset Register are maintained on a day-to-day basis by the Technology Department.

The asset register is updated on three principal occasions, whenever:

- asset procurement;
- asset disposable (especially Leavers, or Asset Retirement processing); and,
- asset allocation or re-allocation (specifically Joiners / Movers processing).

Communications and operation management

Systems and communications services must be operated and maintained correctly.

Systems must be planned for and deployed with regard to the entire security of Walr information assets and the operations of the entire information processing environment.

For sensitive systems separation of duty should be implemented where possible. The following applies:

- Operating procedures should be documented and complied with at all times.
- Technical standards for workstations and mobile devices will be developed and documented.
- The standards will comply with and enforce the ISMS requirements.

Security of Electronic Mail

- Refer to Walr Employee Handbook, E-mail, internet and telephone use

Publicly Available Information

- Formal approval by at least one of the ISMS Owner, Marketing Communications or Sales Team must be obtained prior to any information being made publicly available in any way including media or Internet (web) based.

Acceptable usage policy

Users must not misuse Walr information resources and ensure that Walr's information assets and reputation are protected. Baselines for acceptable use are set out below.

- Users must not attempt to gain unauthorised access to any information resources on the internal or external network
- Users must not engage in activities that may compromise the security of Walr's information assets, nor attempt to break the security mechanisms installed on Walr's computer equipment
- Users must handle company information in a manner appropriate to its security classification
- All information assets in Walr should be protected from damage and safeguarded from theft and unauthorised access or modification
- Walr information resources must not be removed or transmitted from company premises without approval from the owner
- Users shall use only their own user ID to access applications and are accountable for its use; user passwords must be kept confidential
- Staff must not infringe any copyright or other intellectual property rights to information or resources available or retain such information or resources for re-use in any computer system or otherwise
- Staff must ensure that files transmitted into and out of Walr's network, and downloaded to desktops and servers do not pose security risks
- All e-mail and internet communications may be monitored, captured and reproduced without notifying any of the parties involved in the transmission

User password management

Passwords are a common way to verify an identity. Depending on the circumstance, stronger methods such as tokens, smart cards and/or digital certificates may be appropriate. If passwords are used, the following controls must be used:

- Users must keep personal passwords confidential
- When users are required to maintain their own passwords, they must be provided initially with a secure temporary password that they must change immediately
- A process must be in place for password resets. The process should include a user verification procedure (to ensure authenticity of the requestor) and, logging procedure to provide an audit trail
- Temporary passwords provided when users forget their passwords must be changed upon successful logon
- Temporary passwords must be given to users in a secure manner. The use of third parties or unprotected (clear text) e-mail messages to communicate passwords must be avoided
- Passwords should not be stored on a computer system in an unprotected form (i.e., unencrypted)
- Passwords must be alpha-numeric and at least 12 characters in length and contain three of the four following categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
- Default passwords must be changed as soon as possible during or following their initial use, e.g., default passwords are shipped with operating systems and program products for use during system and product installation and setup
- All mobile devices are required to be password protected.

When choosing a password, it is important to select one that you can remember easily, but hard for others to guess. You should avoid using obvious or easily obtained information about yourself or members of your family, such as your name, nickname, date of birth, address, license plate number, email name, etc. Using a word commonly found in the dictionary leaves you vulnerable to intrusion programs that cycle through the dictionary trying each word.

Some possible techniques for selecting good passwords include using multiple unrelated words, using an unusual spelling, imbedding numbers, or punctuation marks inside your password (not at the beginning)

Human resources

People who handle or access Walr information assets must be informed of their responsibilities and be held accountable for using and protecting this information properly.

- All new employees and third parties contracted by Walr should be screened with appropriate background checks completed on a need's basis. The ISMS Owner or relevant manger shall decide whether screening is required.
- A non-disclosure agreement (NDA) or Walr T&Cs should be signed by all parties that have access to Walr information assets.
- Suspected incidents (including security breaches, threats, weaknesses, and malfunctions) that adversely affect the security of Walr information assets must be reported.
- Any changes to an employee's roles and responsibilities must be notified to the Technology department or ISMS owner for a review of their access rights and ensure any movers / shifters are realigned.
- Where possible, segregation of duties should be established to reduce risk of accidental or deliberate system misuse. For systems with financial information or transactions segregation of duties should be enforced.
- All employees must be trained in regard to their roles, in compliance with the Information Security Policy appropriate for their function.
- An on-going information security awareness program must be established to create and maintain security awareness at all staff levels.
- All employees and unsupervised third parties contracted by Walr should be required to assert that they have read and understand the Information Security Policy.

Monitoring and response

Monitoring mechanisms are implemented to identify security trends and detect anomalies. Anomalies should be reviewed to determine if they are indicative of a security event. Events must be reported, investigated, escalated, and corrected to enable a rapid return to normal business operations with minimum damage to Walr information, third-party trust and Walr reputation.

Event Detection and Response

- A Security events response process must be implemented and managed
- All observed or suspected security incidents must be reported to your line manager, a member of the SSC or another senior member of staff immediately to ensure a timely investigation.

In reporting a security incident, relevant information provided may include the following:

- Any evidence of the incident, including the exact text of computer-generated messages
- The scope of the threat, breach, or incident
- Details of any parties involved
- The damage that may have been caused
- The value, sensitivity and criticality of the information or IT facilities affected

When reporting an incident, care must be taken to ensure that no future investigation or evidence is compromised and information about the incident is kept confidential. Any information gathering should be left to the IT department or senior management where the incident is considered significant enough that Law Enforcement is involved.

- Audit trails, application logs and operation system logs must be activated and maintained appropriately to the type of information and its classification
- Retention period of logs must comply with corporate guidelines
- Users of company information resources must be made aware of potential exposures, threats and techniques that may become a security threat

Vulnerability Management

- Vulnerability alerts from various services must be monitored to mitigate exposure to Walr.
- Vulnerability assessment and evaluation of networks and systems supporting Walr business must be conducted periodically and when changes are made.
- Appropriate steps to prevent contamination of, and damage to, computers, applications and information by computer viruses or malicious software must be implemented and maintained.

System acquisition and maintenance

When new systems are proposed, the security aspects of the system should be included in the initial analysis and specification. These specifications must cover automated and manual security measures. A risk assessment should also be performed for significant changes.

Security of System Files

- Change control procedures are required for system files.
- System test data must be protected from unauthorised use and modification.

System Planning and Acceptance

- Capacity planning and monitoring should be implemented to ensure availability of systems and future requirements are managed.
- New systems will have acceptance criteria development prior to selection.
- New systems will be tested prior to acceptance and deployment.

Business continuity management

A business continuity and disaster recovery plan will be formally developed, tested, and maintained for all business resources so as to minimise the effect that a disaster or interruption will have on business.

Business Continuity Planning (BCP) is the documented process or plan designed to enable the business process to continue in the event an asset is destroyed or unavailable.

Disaster Recovery Planning (DRP) is the process or procedure to recover an asset after an event has made the asset unavailable to the business.

It is not the intent of Walr to create a BCP or DRP for every information asset, rather the company views BCP and DRP as a risk management method for protecting its key assets and its service delivery.

Continuity Planning and Testing

- All functions performed by the business and information systems units must be periodically assessed in order to establish criticality of information assets and recovery priorities, and updated to reflect current business activities,
- Business continuity plans must be tested annually.

Information Backup and Recovery

- Information and software must be appropriately backed up and stored remotely to facilitate recovery in the event of a system malfunction or disaster. Appropriate hardware must be put in place and maintained for availability, compatibility, and readiness.
- Restoration of information using the backup information must be tested periodically.
- Backup media must meet the standards of archival, off-site storage and protection as set forth by the applicable business continuity plan.

Physical and Environmental Security

Information assets must be protected by physical security measures and operational processes that safeguard them from theft, misuse, damage, or unauthorised access.

Walr's current baselines for physical and environmental security are to:

- Provide a safe environment by locating computing and network equipment within sites that are not susceptible to man-made hazards or natural disasters, such as fire, water or contamination; implementing controls to limit the effect of such hazards; and designing facilities to protect human safety
- Provide required environment conditioning by meeting hardware requirements for stable and reliable power, air conditioning and ventilation
- Provide necessary physical access controls by restricting physical access to information, software and hardware to those who have a legitimate business need, and by periodically reviewing access requirements and privileges. Physical access to information assets must be limited to appropriate and authorised personnel or those who have a legitimate business need
- Implement emergency procedures by preparing staff to respond effectively in an emergency to protect people and limit damage to information, software or hardware
- Protect the integrity of information transmission facilities by protecting communications hardware and services from interruption and from transmission interception
- Maintain hardware and software records by meeting physical asset control and software license requirements
- Make sure equipment is not removed from the office without the appropriate authorisation
- Ensure that equipment is correctly maintained to ensure its continued availability and integrity
- Ensure that storage devices and materials containing "Confidential" information are physically destroyed or securely overwritten to render the media unrecognisable or unrecoverable prior to disposal
- Information assets classified "Confidential" must be stored in suitable locked cabinets and or other security containers
- Enforce a clear desk and clear screen policy so office desks are cleared of all papers and documents containing material classified "Confidential" or higher when staff leave the office. They will also be clear of all papers and documents classified "Internal" or higher when visitors attend the office.
- Ensure that "Confidential" Information on whiteboards is be erased after use
- Ensure that "Confidential" printouts are cleared from printers as soon as practicable
- Ensure that system information and designs are kept secure and classified as "Confidential" Any use of third-party properties or services to support company operations should be thoroughly reviewed and assessments completed for suitability (i.e. Data Centres or storage locations).
- All physical and environmental controls should be considered and aligned, managed and reviewed in line with the Walr Supplier Management Policy.

Visitors

- All visitors to the office should be recorded.
- Visitors include all guests including contractors, consultants, tradespersons, cleaners or any other person not directly employed by Walr.
- Visitors must be escorted at all times. The exceptions to this are trusted individuals who may be left unescorted on approval of one of the senior staff, and on the condition that an NDA has been signed by the visitor.

Cryptography

Encryption Baselines

Walr's information assets shall be appropriately protected to prevent unauthorised access by applying a level of encryption to information classified as Internal or above:

- All Walr -owned data when in transit outside of Walr 's internal network;
- All removable media, e.g. USB drives, thumb drives, memory stick etc;
- Laptop hard drives;
- All wireless networks carrying such information; and
- Emails (including attachments).

Encryption as per Classification

All information assets classified as Internal or above must be encrypted. Information assets which are not classified as Internal or Confidential must still be considered for encryption if it is considered necessary for adequate security.

Encryption of Data in Transit

Internal & Confidential data in transit must always be encrypted. Data, which is already in the public domain, can be sent unencrypted.

Key Management

Software which force-encrypts removable media employs its own key management system.

Encryption keys must be securely managed in accordance with documented procedures.

Security compliance

Compliance with company policies and legal requirements is required to assure that Walr information assets, including those entrusted to Walr by third parties, are protected from misuse, disclosure, theft, or loss.

Compliance with statutory, regulatory, and contractual requirements

- All compliance requirements shall be defined, and processes developed to ensure compliance
- Customer information must be protected with logical and physical access controls, including controls to authenticate and permit access only to authorised individuals and only for permissible and authorised uses.
- Legal and regulatory requirements must also be complied with when sharing information with non-affiliated companies
- Any new projects should consider information security and compliance requirements.

Third Party Security Compliance

- Security risks associated with externally supplied services must be mitigated to an acceptable level. Third-party service providers are required to meet all relevant Walr security policies, and specific provisions for oversight and compliance are to be integrated into all third-party contracts.
- Appropriate due diligence must be exercised in selecting service providers
- Contracts must ensure that service providers comply with the Walr Information Security Policy, including use, disclosure, and protection of consumer information.
- As appropriate, service providers must confirm that they have satisfied their obligations as required by these policies. Audits or other equivalent evaluations of their compliance must be performed, and results reviewed.
- Third parties must not share “Internal or Confidential” information with non-affiliated companies, unless explicitly approved by the relevant authorised party in Walr.

Self-Assessment and Monitoring

Periodic self-assessments of security practices should be conducted. Key controls, standards, and procedures necessary to comply with these policies must be reviewed and tested annually at a minimum. Documentation of the annual test must be retained for an audit review.

New products and services, including those provided by third parties, must be tested before being placed in production to ensure that security controls are properly designed and implemented.

Privacy and Monitoring

The Company reserves the right and may periodically monitor use of company hardware and software, including the content of email, documents, telephone messages, images, and graphics in accordance with local legislation.

By using company equipment, each employee acknowledges:

- that they have no reasonable expectation of privacy,
- that they consent to monitoring of their use of Company Equipment without prior notice to the employee; and
- that assignment of initial passwords by the Company for use of computer, telephone or other Company Equipment, and any subsequent changes of passwords by the employee, do not create an expectation of privacy or alter any of the employee's acknowledgements concerning monitoring by the Company.

Failure to comply with any of the above is considered a breach of policy and will result in disciplinary action up to and including dismissal.