

Information Security Policy

Date	Name	Role	Change	Version
Tue Sep 12 2023	Scytale System	Scytale System	Created	V0.1
Thu Feb 22 2024	Yuval Abadi	COO	Approved	V1.0

Information Security Policy

General

The Information Security Policy serves as the foundation for all the Lasso's Global Information Security and Privacy activities, and as a guide for implementing practices to minimize risk to the Lasso's operations.

This Policy has been created to define the methods with which Lasso protects and secures data, that Lasso receives.

Purpose and Scope

This document outlines Lasso's Information Security Policy. This security policy describes Lasso management's view of information security and its implementation in both corporate vision and day-to-day activities of the company. The security policy provides the high-level guidelines for practicing information security in Lasso. Further details regarding the implementation of various information security aspects can be found in Lasso's matter-related policies.

This security policy relates to Lasso's activities worldwide. The policy refers to all systems, networks, and data resources operated and managed by Lasso.

Information Security is essential to Lasso's business because:

- It helps maintain a reliable service.
- Achieving and maintaining compliance with various laws and regulations in the countries in which Lasso operates in.
- It helps protect Lasso's clients and their information.
- Complying with Customers' and Regulators' security requirements.
- Managing and reducing risk to Lasso's activities.

Lasso's management is committed to **maintaining a high level of information security** and intends to invest the required resources to enforce its security policy in all aspects of Lasso's activities.

All Lasso employees, consultants, contractors, and affiliates are subject to the policies noted herein. Continued lack of adherence to the policies may result in appropriate disciplinary action, up to and including termination of employment or affiliation.

Roles & Responsibilities

Responsibility to follow this policy applies to all Lasso employees.

The CISO/COO is responsible for developing, maintaining, and implementing the Information Security Policy.

The roles and responsibilities of the respective employees at Lasso are set out in the Roles and Responsibility Policy.

Policy Framework Details

Lasso's current business strategy and framework for information security are the guidelines used for identifying, assessing, evaluating and controlling information-related risks, through establishing and maintaining the Global Information Security Policy (this document).

Lasso management has decided that information security is to be ensured through application of the policy for information security, and a set of underlying and supplemental documents (such as security procedures and

guidelines). In order to secure operations at Lasso, Lasso shall ensure the availability of continuity plans, backup procedures, defense against damaging code and malicious activities, system and information access controls, incident management and reporting, even after serious incidents.

The term **Information Security** is related to the following basic concepts.

- **Confidentiality:** The concept that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** The concept of safeguarding the accuracy and completeness of assets.
- **Availability:** The concept of information and assets being accessible and usable upon demand by an authorized entity.

Security Goals

- Lasso is committed to safeguarding the confidentiality, integrity, and availability of all physical and electronic information assets of Lasso, to ensure that regulatory, operational, and contractual requirements are fulfilled.
- Lasso will define the policy of management and handling of cyber incidents in the company and anchor the management's concept of implementing a cyber-threat security program.
- Lasso will provide guidance, support, and documentation of management's commitment to implementing information security through awareness to all relevant parties.
- Lasso will handle the integration of cybersecurity in the business and operational aspects of the organization, including at the strategic planning and operational level of the organization.
- Lasso will develop and Implement information security and privacy programs in the organization.
- Lasso will conduct cyber threat research and detect exposures and risks that exist on information assets and computing systems in the organization that can cause damage to their proper operation (such as downtime, deletion, destruction, unauthorized change, etc.).
- Lasso will review on a regular basis the existence of cyber security and privacy programs in the organization, learn and apply them.
- The overall goals for information security of Lasso are as follows:
 - Ensure compliance with current applicable laws, regulations, and guidelines.
 - Comply with requirements for confidentiality, integrity, and availability for Lasso's employees, customers, business partners, and other users.

- Establish controls for protecting the Lasso information and information systems against theft, abuse, and other forms of harm and loss.
- Motivate administrators and employees to maintain responsibility for, ownership of, and knowledge about information security, in order to minimize the risk of security incidents.
- Ensure that the Lasso is capable of continuing its services even if major security incidents occur.
- Ensure the protection of personal/sensitive information/data (privacy).
- Ensure the availability and reliability of the network infrastructure and services supplied and operated by Lasso.
- Comply with methods from international standards for information security and privacy, SOC 2, ISO27001, PCI DSS, GDPR.
- Ensure that external service providers comply with the Lasso Information security and privacy needs and requirements.
- Ensure flexibility and an acceptable level of security for accessing information systems remotely.

Laws and Regulations

Lasso undertakes to comply with the laws and regulations governing the processing of personal data/data privacy where Lasso operates, including, but not limited to, GDPR, PCI DSS, ISO27001, SOC2, and any other national applicable laws or regulations governing the processing of personal data and data privacy.

These laws and regulations have an impact on data management, for example, backup requirements of accounting systems, data retention of employee data, and more. The legal department is responsible for the identification of new relevant laws and changes to existing laws.

The CISO/COO monitors the evolution of technology currently in use by Lasso, as well as information security risks.

Intellectual Property

Users must not make unauthorized copies of software owned by the organization, except in cases permitted by law, by the manufacturer, or the legal department.

Users must not copy software or other original materials from other sources and are liable for all consequences that could arise under the intellectual property commitments, as applicable by law or other company policies.

Information Security Policy

- Security Organizational Structure: Information Security responsibility and authority in Lasso is delegated by CISO/COO, assumed responsibility as Lasso's [Chief Information Security Officer (CISO)]. Along with the CISO/COO, a [Security Steering Committee] will act as an advisory board and a channel to communicate security issues from and to the CISO/COO.

The roles and responsibilities of the CISO/COO at Lasso are set out in the Roles and Responsibility Policy.

- The CISO's duties will include:
 - Defining Lasso's information strategy and requirements.
 - Setting, prioritizing, and managing Lasso's information security initiatives.
 - Updating and reviewing Lasso's information security policy.
 - Setting the information security standards for Lasso networks and systems.
 - Recommending security enhancements and features for Lasso's products and services.
 - Defining and managing ongoing security auditing and testing processes.
 - Defining required security mechanisms and managing their implementation.
 - Managing information security incident response.

- Managing security-related discussions with clients and other 3rd parties.
- The CISO will report directly to the CTO and the board of directors.

Security Forum/Steering Committee

The Security Steering Committee will act as an advisory and review board to the CISO. The committee will provide a broader view of the company's requirements and goals, by including representatives from various departments which have interfaces to information security.

The roles and responsibilities of the Security Steering Committee at Lasso are set out in the Roles and Responsibility Policy.

- Review security activities performed in the past quarter and planned activities for the next quarter.
- Review and approve changes to this policy (annually).
- Review and approve the information security work plan (annually).
- Review information security incidents, their management, and lessons learned from them.

Responsibility and Ownership for Information Assets

- Lasso maintains a current list of all its information assets.
- Each and every information asset belonging to Lasso is owned by an information asset owner. The owner of each information asset will be determined by the CISO/COO, with the assistance of the relevant Business Owner. An information asset owner can be only an internal Lasso employee.
- Changes in ownership will be allowed only when approved by the CISO/COO.
- An information asset owner assumes the following responsibilities:
 - Determining the sensitivity level of the information asset.
 - Determining the criticality level of the information asset.
 - Determining the risk level of the information asset.
 - Determining the type of data stored on the information asset.

- Promoting awareness of the security characteristics of the information asset.

Information Classification and Sensitivity

- All Lasso information is categorized into four main classifications: Public, Internal Use, Confidential and Restricted. If an employee is uncertain of the classification of a particular information asset, he/she should contact their direct manager or the CISO/COO.
- Public Information: The information is public and can be shared openly on a website, discussed publicly, and shared with any individual. The use of public information requires no additional control because it is inherently public.
- Internal Use: Internal information is company-wide and should be protected with limited controls. Internal information may include the various policies, knowledgebase, and the company's internal communication. Disclosing internal information will have only a minimal impact on the business.
- Confidential information: Information that is confidential should be used within the organization as a whole. Marketing materials, pricing, and contact details are examples of such information. In the event that Confidential information is disclosed, the company's reputation and profitability could be negatively affected.
- Restricted information: Restricted information is highly sensitive and its use should be limited on a need-to-know basis. In most cases, restricted information is protected by an NDA to minimize legal risks. Trade secrets, Intellectual property, personal information, financial details, health information, or customer data are considered restricted information. If disclosed, there would be a significant financial or legal impact on the business.
- The proper way to allow access, protect, distribute and dispose of the information belonging to the various sensitivity levels can be found in the "Data Classification Policy".

Disaster Recovery

- The Disaster Recovery Policy provides the framework for the Disaster Recovery Plan to be implemented by Lasso in order to mobilize its response and undertake work to prevent or mitigate the severity of potential disruptions.
- The Plan will identify the recovery objectives, the structure for implementation, mitigation measures, and the communication process to

keep staff, partners, and the public informed of necessary changes to service delivery.

- Further information regarding business continuity can be found in the “Disaster Recovery Policy”.

Risk Assessment

The Company shall continuously assess the risk and evaluate the need for protective measures. Measures shall be evaluated based on their criticality and with regard to efficiency, cost and practical feasibility. An overall risk assessment of the critical information systems shall be performed annually.

Risk assessments shall identify, quantify and prioritize the risks according to relevant criteria for acceptable risks.

Risk assessments shall be performed when implementing changes that impact information security and privacy. Recognized methods of assessing risks shall be employed.

In the event that new technologies are introduced that potentially could result in a high risk to the rights and freedoms of natural persons, the Company will perform a Data Protection Impact Assessment (DPIA) to determine the impact of the envisaged processing operations on the protection of personal data.

Select appropriate information security risk treatment options, taking into account the risk assessment results. Determine the controls that are necessary to implement the information-selected security risk treatment options. Formulate an information security risk treatment plan.

Obtain risk owners’ approval of the information security risk treatment plan and acceptance of the residual information security risks. Risk management shall be performed according to criteria approved by the Company management.

Risk Treatment

The CISO/COO shall be responsible for maintaining security controls for all Lasso assets, locations, employees, risk managements, and process. A risk treatment plan shall be provided that includes the resources, responsibilities, and priorities, together with action taken by Lasso management towards the risk identified. These shall be documented, implemented and reviewed periodically by the CISO/COO.

A risk treatment plan shall be prepared, specifying the technology and the process controls that are to be implemented. The plan shall be presented to the Management team for approval. Senior management shall review the approach and the solution, which includes steps to be taken to mitigate a particular risk, and shall approve the treatment plan.

The Information Security team shall be equipped with sufficient knowledge to ensure that they are able to implement the required controls with the required effect, and to maintain information security to the fullest extent.

ISMS operations shall be led by the Information Security Team with the assistance of other Lasso departments such as Development and Infrastructure teams. The roles and responsibilities of all involved personnel are defined in the "Roles and Responsibilities Policy".

The effectiveness of all security controls is measured and, if effectiveness found to be low, actions are taken accordingly. The effectiveness and meeting of security objectives are measured through analysis of relevant logs and records, such as incident reports, access logs, network logs, Business Continuity tests, formal risk assessments and penetration tests based on the annual work plan.

The Statement of applicability ("SOA") of the ISMS and PIMS implementation shall be prepared and approved by the CISO/COO.

The Statement of applicability ("SOA") shall enlist the controls according to the ISO 27001 and 27701 standards, the applicability/implementation status together with a statement based on their selection or omission.

Malware Detection and Response

This procedure defines the process for detecting and responding to viruses, trojans, malware, and ransomware in Lasso's workstations and production systems. Further information can be found in the "System and Network Management policy".

Service Disruption Communication

This process defines the communication procedure for service disruption incidents. The process is designed to achieve the following goals in case of critical Service Disruption incidents:

- Provide near-instant initial notification to impacted customers and internal stakeholders.
- Ensure an ongoing communication channel as long as corrective measures are being taken.
- Deliver a clear postmortem analysis to customers and internal stakeholders following resolution of the incident.

Further information regarding service disruption communication can be found in the "Incident Management policy".

Penetration and vulnerability tests

- Lasso performs penetration tests on an annual basis. Vulnerability scans are performed regularly on the production network, and staging network.
- Vulnerability scans can be performed following a major release deployment, or on a regular basis and at least daily. A "Major Release" is defined as a significant addition to or overhaul of the Lasso platform.
- Web-application penetration test can be performed following a major release deployment or on a quarterly basis. Critical/high issues must be remediated in a timely sensitivity. A re-test report should be performed to examine suitable remediation of identified critical and high issues.
- Source code analysis will be performed on code before it is sent to production. Code will be tested in the staging environment.

Service Level Agreement

Lasso's Service Level Agreement can be found as a part of the Master agreement signed between Lasso and the client. In case the company did not provide a Service Level Agreement ('SLA') as part of the Master Agreement, it will monitor the target SLA for internal use only.

Access control

- Access to Lasso information assets are restricted and will be granted to Lasso employees and contractors in order to fulfill their duties on a need-to-use basis. Lasso employees and contractors will not be granted access to

any information asset that is not directly needed to their work in Lasso with consideration to segregation of duties ('SoD').

- Lasso has defined various user roles, according to the various positions and activities in the company. Each Lasso employee and contractor will be assigned one of these roles and receive access control privileges relevant to that role, in accordance with its roles and responsibilities.
- Access requests need to be considered and approved by the business owner and Asset custodian prior to access provisioning. All the access requests are documented in the internal systems.
- Further information regarding access control can be found in the "Access Control policy".

Accountability

- Each Lasso user is personally accountable for his/her actions regarding Lasso information assets and device.
- Any Lasso user that will not comply with Lasso's information security policy shall be personally responsible for this non-compliance and subjected to sanctions elaborated in the Code of Conduct and as the law permits.

User account management

- Each user in Lasso shall receive a personal user account. This user account shall be used by the user it was assigned to and only by that user. Users shall not allow other users to use their personal user account or use user accounts of other Lasso employees.
- Generic accounts (accounts that do not belong to a specific user, but rather serve a group of users) are not acceptable, as they prevent accountability for actions performed under that account. In case Generic Accounts are critical to the operation of Lasso's service, they should be documented and approved by the Business Owner.

User authentication

- Users are required to log in to Lasso's production servers in order to access their user accounts. Logging into Lasso's system requires the users to authenticate themselves. The authentication method used depends on the sensitivity of the information asset, the authorization level requested by the user (e.g. regular user, administrator), and the access method used (e.g. internal network, remote access).

- Authentication data and devices (e.g. passwords, authentication tokens) provided by Lasso are meant for the individual use of the user receiving them. Authentication data should not be given to any other party or used in any way other than for the fulfillment of the user's duties.

Audit

- The use and activity of Lasso information assets are logged for audit trail.
- The logged data is audited for security and non-compliance with Lasso's information security policy and additional procedure.
- Lasso's Security Steering Committee performs an annual review of the information security policy and the company's compliance with the various policies. This review outlines potential issues, proposed changes, and improvements.

Reporting

- Each security-related event that is detected by any Lasso employee or system is reported to the relevant information asset owner and to the [CISO/COO].
- The CISO/COO compiles annual reports of information security activity and information security events and presents them to the Information Security Committee when it convenes.

Incident response

- Security incidents detected by Lasso employees, clients, or business partners shall be reported to the CISO/COO.
- The CISO/COO will guide the relevant IT and/or Operations personnel in performing the required forensics, mitigation, and improvement activities for each security incident.
- The CISO/COO shall report all security incidents and the lessons learned from them to the Security Steering Committee.
- Further information regarding service disruption communication can be found in the "Incident Management policy".

Security Awareness and Training

- Managers shall ensure that staff and external parties who are working with systems and data are formally aware of, and educated about, the security and privacy policies and procedures with which they must comply. This step is fundamental to establishing individual accountability.
- All users within the scope of this document shall receive appropriate awareness and training and regular updates about Lasso policies and procedures, as relevant for their job function.
- Security awareness is a key factor in maintaining a high level of information security in Lasso.
- Each employee receives an information security briefing upon commencing work in Lasso. The CISO/COO provides Lasso employees with security awareness materials and training on an annual basis.
- The CISO/COO may also notify Lasso employees when information security incidents that have a major impact on its products and services have occurred. These case studies are used to provide a better understanding of information security and enhance the security level of future software versions.
- Further information regarding Security Awareness and Training can be found in the "Security Awareness and Training policy"
- For additional information regarding Security Awareness, refer to Security Awareness Training Procedure.

Communication Security and Perimeter protection

- Lasso's network and information assets are surrounded by the Lasso perimeter. The perimeter is implemented using various communication and security technologies and mechanisms (e.g. firewalls, routers, security groups).
- The perimeter prevents unauthorized access to Lasso information assets by external entities and prevents leakage of Lasso information assets to the outside world.

Communication Security and Network Segregation

Lasso's network is divided into three segregated network environments: The development environment, the staging environment, and the production environment. Each of these environments is segregated from the other environments and has its own privilege allocation and access control.

Communication Security and Limited Access by External Entities

- Access to Lasso's information assets by external entities are restricted. Only specific access that is essential to the successful operation of Lasso's service is allowed.
- All access by external entities is pre-approved by the CISO/COO. Any change to the external-access status is reported to the Security Steering Committee by the CISO/COO.

Communication Security over external channels

- All communication based on external channels (e.g. the Internet) transferring Lasso confidential information is encrypted using standards-based encryption technology. This communication is encrypted between the Lasso production environment and Lasso remote computers.
- The use of encryption is subject to the relevant governing laws and regulations in each country Lasso operates in.

Communication Security and Remote Access

- Remote access to Lasso's networks or information assets are restricted and are allowed to a limited group of Lasso employees that require remote access in order to fulfill their duties.
- Remote access to Lasso's information assets are limited to the absolute minimum of services and data assets necessary for the proper work of Lasso's service and its maintenance.
- All remote access to Lasso's networks or production information assets are conducted using VPN mechanisms.

Human Resources Security

- All prospective employees go through pre-employment reference and/or background checks, according to the HR policy.
- All employees sign confidentiality and/or NDA agreement, Code of Conduct, and Acceptable Use policy when their work commences.

- Any change in an employee's position in Lasso or change in his/her access privileges is reported to the direct manager and the HR.
- Termination of an employee's employment is reported to the direct manager and HR, who verifies that all of the employee's access privileges and authentication data have been revoked, relevant documentation signed and all assets returned.

Security in the Development Process

- Information Security aspects are considered in every phase of the development lifecycle, from the initial requirement, design, coding, testing, and final deployment.
- Security testing is performed as part of the coding process throughout the development lifecycle, according to the "SDLC Policy".
- Software development and SDLC change management in Lasso is performed according to the "SDLC policy".

Change Management

Lasso's services and networking environment are dynamic, to support the changing needs of its customers and the ever-growing requirement for capacity and performance. Changes to Lasso's services or networking environment (excluding regular patching and updating processes) might require security clearance from the CISO/COO. This process is described in the "Change Management policy".

Physical Access Controls

- Lasso hosts its data in AWS. Lasso manages its data center activities in a highly secured environment, with strict access controls (both logical and physical). Servers at the data center are in a secure location with security measures implemented to protect against environmental risks or disasters and performed by AWS. Lasso review security examination reports (such as SOC 2 Type II) on an annual basis.
- Further information regarding Physical Security related matters can be found in the "Physical Security policy".

Asset Management and Classification

Lasso will maintain an inventory of all its information assets, regardless of their physical and geographical location. All assets will be classified, to ensure that all information receives the appropriate level of protection, including encryption and hardening when required.

As part of the maintenance of the Records of Processing Activities, Lasso will map the private data related to its processes, including a description of the categories of data subjects and of the categories of personal data (including, but not limited to, special categories of personal data, e.g. a person's race, age, political opinions, religion, sexuality, genetic info, biometrics, children information)

All Company IT assets (such as data, software, hardware, etc.) shall be accounted for and have an owner. IT asset owners shall be identified for all assets and shall be responsible for the maintenance and protection of their assigned assets. All information shall be classified and handled according to its sensitivity levels. For additional information regarding the Company data classification process, refer to Data Classification Policy. For additional information regarding the Company inventory of assets stored in the cloud, refer to Asset Management Policy.

Acceptable use

- The use of Lasso's network and all information assets and systems are subject to Lasso acceptable use policy.
- Use of Lasso's Email and instant messaging systems are subject to Lasso acceptable use policy. Any use of external systems to process or transmit Lasso information is subject to this information security policy and the acceptable use policy.
- All new and existing users should be aware of the acceptable use policy and accept it prior to using Lasso's network, information assets, and systems.
- Further information regarding acceptable use can be found in the "Acceptable use policy".

Verification and Measurement

- Lasso's management verifies and measures its security status versus its security targets.
- Verification and measurement are performed by:
 - Reviewing security project plans vs. actual implementation.

- Analyzing the number and severity level of information security incidents compared to the previous year.
- Yearly external audit.

Cryptographic Usage

Cryptographic usage applies to all Company employees and affiliates and covers acceptable encryption techniques for various types and states of data.

To ensure correct and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information, Lasso will ensure that:

- Data in motion will be encrypted using secure protocols when transmitted to third parties, in accordance with the Company's data classification policy.
- Confidential data, as defined by the Company's classification policy, will be encrypted whenever extracted from their primary repository.

For additional information regarding the cryptographic usage policy, refer to the Encryption key management Policy.

Supplier Relationships

The Company will ensure that its partners, suppliers and contractors will maintain adequate security measurements to secure Lasso's and its customers' information, through contracts and periodic audits as necessary.

The Company shall develop guidelines and conduct third-party security assessments prior to signing contractual engagements, in order to ensure protection of the Company's assets that are accessible by those third parties.

The Information Security team shall ensure that external parties follow the Service Level Agreement (SLA), Code of Conduct, Non-disclosure agreement, and security and privacy policies for addressing the security and privacy risks to the Company's information and information processing facilities, if logical/physical accesses are granted to the external parties in future.

Risk assessment exercises shall be performed according to the procedures specified by the Information Security manager to identify security and privacy risks.

For additional information regarding the security processes for working with third parties, refer to Third Party Security Policy.

For additional information regarding the physical control process, refer to Physical Security Policy.

Operations and Communications Security

The Company shall maintain appropriate controls related to management of corporate IT, including change management, capacity management, malware, backup, logging, monitoring and vulnerabilities management. The Company shall maintain appropriate controls related to communication security, including network security, segregation, network services, transfer of information and secure messaging. The Company shall operate processing facilities securely.

Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities shall be established. Appropriate operating procedures shall be implemented. Segregation of duties shall be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse. The capacity management of existing systems, and the process for integrating new systems within the Company, shall be conducted according to Company policies. A change management process shall be established to ensure that changes are well controlled. For additional information, refer to Change Management Procedure.

A patch management process shall be established to ensure that patches and updates are well-tested before deployment and installation. For additional information, refer to Vulnerability and Patch Management Procedure. For additional information regarding communication, refer to System and Network management Policy.

Information Sharing

The organization must define, develop and implement information sharing processes within the organization (with internal parties) and outside the organization (with external parties such as CISO Forums).

Secure System Development Lifecycle

The information security requirements for new information systems or changes to existing information systems shall be defined during the development of business requirements.

Controls to mitigate any identified security and/or privacy risks shall be implemented where appropriate.

The Company has adopted the “Privacy By Design” and “Privacy By Default” principles in its Secure Software Development Life Cycle (S-SDLC)

For additional information regarding the software security processes, refer to S-SDLC Policy.

Information Security Incident Management

The Company will ensure that all employees work to prevent information security incidents from occurring. Should an incident occur, the Company will swiftly implement appropriate actions.

In the event of privacy breaches that have exposed or damaged personal information, the proper authorities will be notified within 72 hours of Lasso becoming aware of them.

In the event of privacy breaches that carry a high risk of harm to data subjects, the data subjects will be notified without undue delay. Information security incidents and discovery of vulnerabilities associated with information systems shall be communicated in a timely manner. Appropriate corrective actions shall be taken. Formal incident reporting and escalation shall be implemented.

All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of security or privacy incidents, or vulnerabilities that might have an impact on the security of the Company's assets. Information security incidents and vulnerabilities shall be reported as soon as possible to the Security department.

In the event that a follow-up action against a person or Company following an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules of evidence laid down in the relevant jurisdiction(s). Depending upon the type of security incident, the physical or technical evidence shall be retained for future legal purpose and provided to the operational people for further course of action.

For additional information related to the Company's Information Security Incident management activities, refer to Security Incident Management Policy.

Compliance

The Company shall abide by any law (statutory or regulatory) or any contractual obligations affecting its information and information systems.

The design, operation, use, and management of information systems shall comply with all statutory, regulatory and contractual security requirements.

Lasso recognizes the need to keep the information security environment current on an on-going basis. To achieve this goal, it has implemented the following:

- Periodic review of the security policy.
- Periodic updates regarding the versions, patch levels.
- Periodic penetration test and Vulnerability Assessment.
- Ongoing tracking of security related tasks to closure.
- Build education and awareness through new channels.
- Improve software security related to all client's connection and information transfer.

Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. Organizational records shall be categorized into record types, e.g. database records, transaction logs, audit logs, operational procedures each with details of retention period and type of storage media (e.g. paper, optical media, magnetic media, etc.).

The Company will identify compliance requirements, including contractual, regulatory and legal requirements, and shall integrate them into the Information Security Program as required.

[The Company is committed to complying with best security practices and relevant regulations such as the General Data Protection Regulation (GDPR).]

The Company will conduct internal audits at defined intervals, to provide data about the effectiveness of the information security management system.

System Acquisition, Development and Maintenance

Lasso will maintain security throughout the lifecycle of the information systems.

Lasso will consider security and privacy during system or software analysis and design and will implement appropriate measures, designed to implement data-protection principles, such as data minimization, in an effective manner and will integrate the necessary safeguards into the processing in order to protect the rights of data subjects. (Data protection by Design and by Default).

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

Lasso will implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Cloud Services

Information stored in the cloud computing environment shall not be subject to access and management by the cloud service provider other than as legally required, and for maintaining the cloud provider services and providing them to the Company's customers and their end users. Assets may be maintained in the cloud computing environment, e.g., application programs.

Segmentation shall be enforced, based on cloud provider services segments. Hardening shall be enforced according to CISO best security practices. A complete logical segregation shall exist between customers' data within the Company's environment.

Administrative access to the production environment shall be granted on a need-to-know basis. For additional information related to privileged access to cloud service administrators, refer to Access Control Policy. The Company shall identify the authorities relevant to the combined operation of the cloud service customer and the cloud service provider.

For additional information regarding the Company's inventory of assets stored in the cloud, refer to Asset Management Policy.

Continual Improvement

Lasso's management strives for continuous improvement in its information security status. Each Security Steering Committee meeting includes a review

of improvements performed in the previous quarter and a discussion of further potential improvement.

Document Ownership

The COO is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with Lasso's review requirements. A current version of this document is available to all members of staff in the company Shared Drive, Folder.