konaAI

IT Security Policy

Policy & Standards

Product Development

Team, Kona AI

INTRODUCTION

This policy defines the high-level objectives and implementation instructions for Kona AI information security program. This policy also defines management roles and responsibilities for Kona AI Information Security Management System (ISMS). Finally, this policy references all security controls implemented within the organization.

Within this document, the following definitions apply:

- Confidentiality: a characteristic of information or information systems in which such information or systems are only available to authorized entities
- Integrity: a characteristic of information or information systems in which such information or systems may only be changed by authorized entities, and in an approved manner.
- Availability: a characteristic of information or information systems in which such information or systems can be accessed by authorized entities whenever needed.
- Information Security: the act of preserving the confidentiality, integrity, and availability of information and information systems.
- Information Security Management System (ISMS): the overall management process that includes the planning, implementation, maintenance, review, and improvement of information security.

PURPOSE

The objective is to protect the confidentiality, integrity, and availability of Kona AI information, the supporting IT systems, business processes, client, and personal data.

- This information security policy defines the purpose, direction, principles, objectives, and basic rules for information security management.
- This document also defines procedures to implement high level information security protection within the organization, including definitions, procedures, responsibilities, and performance measures (metrics and reporting mechanisms).

SCOPE

This policy is applicable to Kona AI corporate and regional offices, physical information assets, information processing facilities and all other pertinent physical elements near the facility.

This policy applies to all facilities and administrative functions across KonaAI.

This Policy applies to Kona AI Group- to all users of information systems within KonaAI. This typically includes employees and contractors, as well as any relevant external parties that use systems and information controlled by Kona AI (hereinafter referred to as “users”). This policy must be made readily available to all users.

The information security policy (or policies) lays out and confirm senior management's commitment to:

- The organization's information security objectives
- Continuous improvement of the ISMS

Some of the other things that top management needs to do around this clause beyond establishing the policy itself include:

- Making sure it is relevant to the purpose of organization.
- Clarifying the information security objectives
- A commitment to satisfy the applicable requirements of the information security needs of the organization.
- Ensuring its ongoing continual improvement – an ISMS is for life, and with surveillance audits each year.
- Sharing and communicating it with the organization and interested parties as needed.

1.0 MANAGEMENT DIRECTION FOR INFORMATION SECURITY

Reference: ISO/IEC 27002:2013 || A.5.1

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A management framework shall be established to initiate and control the implementation of information security within Kona AI. Management will approve the information security policy, clearly define, and assign security roles, and coordinate and review the implementation of security controls across the organization.

The policies of information security will be reviewed at planned intervals and will be communicated to employees and relevant external parties.

Senior management may prefer to mandate a single, succinct, broad/overarching governance-type policy (formally satisfying the ISO requirement), supported by a suite of detailed information risk, security, compliance, privacy and other policies, procedures, guidelines etc.

1.0.1 Policies for Information Security || A.5.1.1

A set of policies for information security shall be defined, approved by KonaAI management, published, and communicated to employees and relevant external parties.

1.0.2 Review of the policies for the information security || A.5.1.2

The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

1.2 Information Security Program Objectives

The organization's main objectives for information security include the following:

- Reducing the likelihood of security incidents.
- Reducing the damage caused by potential incidents through effective response to security incidents by containing the impact and eradicating the cause in a timely manner.
- Identify and manage risk to information security down to a tolerable level and continually improve the security capability.
- Implement a standard, consistent and repeatable measurement of risk.
- Ensure information security control effectiveness and embed information security within project and change activity.
- Perform information security due diligence on third parties to identify and manage risk; provide assured responses to 3rd party due diligence data requests.
- Provide consistent and effective security awareness training for every member of staff via co-ordinated delivery methods to ensure understanding.
- Perform independent information security testing on external facing and internal critical business systems to help ensure protection against compromise.
- Creating a better market image and provide KonaAI with a competitive advantage.

These goals are in line with Kona AI's business objectives, strategy, and business plans. The CISO is responsible for reviewing these general ISMS objectives and setting new ones.

Objectives for individual security controls or groups of controls are proposed by the Security Management Team and approved by the CISO.

Kona AI will measure the fulfillment of all the objectives. The CISO is responsible for setting the method for measuring the achievement of the objectives – the measurement will be performed at least once a year and the CISO will analyze and evaluate the measurement results and report them as input materials for the Management review.

All objectives are reviewed at least once per year. This exercise is coordinated by the Info-sec Team. The results are then analyzed, evaluated, and reported to the management team to draw an implementation plan.

1.3 Responsibilities

Responsibilities for the ISMS are the following:

- The CISO is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available.
- The CISO is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS.
- The CISO is responsible for obtaining business commitment and support for the ISMS as detailed within the RACI contained in the Appendix of this document.
- The Information Security Forum must review the ISMS at least once a year or each time a significant change occurs and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy, and effectiveness of the ISMS.
- The CISO will implement information security training and awareness programs for employees. Evidence of the training provided must be retained as part of the implementation of the ISMS and for audit purposes; access to the evidence must be based on a business need.
- The protection of confidentiality, integrity, and availability of assets is the accountability of the owner of each asset.
- All employees, contract, temporary and third-party staff working for and on behalf of KonaAI, as well as relevant external parties have responsibility for maintaining full adherence to KonaAI's policies and procedures, ensuring all information held is accurate and kept confidential.
- All employees, contract, temporary and third-party staff working for and on behalf of KonaAI as well as relevant external parties must ensure any act or omission which could lead to an information security breach is reported in line with the standard incident reporting procedure.
- All security incidents or weaknesses must be reported to the CISO in a timely manner in accordance with the KonaAI incident management procedures.
- The CISO will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when in accordance with the current relevant legislation.
- The CISO is responsible for adopting and implementing the Information Security Training and Awareness Plan, which applies to all persons who have a role in information security management.

2.0 DECLARATION OF SUPPORT FOR ISMS IMPLEMENTATION

The Management at KonaAI is committed to establishing a strong culture of information security by building a robust information security management system (ISMS). The ISMS shall address the information security needs of the organization, its employees, suppliers, service providers, stakeholders, sub-contract workers, dealers, and channel partners. We are committed to provide the necessary guidance and resources needed to design, implement, and monitor an ISMS, meeting the needs of the organization.

- Protection of the organization shall be at the root of our information security practices.
- Committed to secure the information of our employees, customers, partners, suppliers, and other relevant stakeholders in all its forms.
- Ensure that information assets are protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional.
- Creating awareness on the importance of information security among interested parties
- Committed to provide adequate resources to implement and sustain an effective information security management system for the organization.
- Continually assessing and managing the risks involved
- Complying with legislative, regulatory, and contractual requirements for information security.
- To establish well defined process controls using latest technologies and tools for continual improvement of the information security management system.
- Developing and implementing Business Continuity Plans

This Policy is supported by the following high-level objectives:

- Implementation of a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001 Standard for Information Security Management Systems
- Implementation of an Information Security Risk Assessment Process that assesses the business harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and controls currently implemented.
- Development and implementation of a Business Continuity Plan to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters (Ref: Business Continuity Policy)
- Defined security-controlled perimeters and access to controlled offices and facilities to prevent unauthorized access, damage and interference to business premises and Information security awareness guidance for all company employees.
- A Senior Management Team that supports the continuous review and improvement of the company ISMS
- Implementation of incident management and escalation procedures for reporting and investigation of security incidents for ISMS management review and action

The company information security policy is reviewed by the Senior Management Team every 6 months as part of the management review, who recommend amendments and updates to the policy, as part of the continuous service improvement process.

This policy will be made available to Interested Parties, where required.

All managers' head of the functions are responsible for implementing the policy and ensuring staff compliance in their respective business functions. The head Leader of the function and CISO shall interact on an ongoing basis to measure the effectiveness of ISMS.

The Management at KonaAI is committed to the Information Security Management System (ISMS), and shall ensure that information security policy is communicated, understood, implemented, and maintained at all levels of the organization and regularly reviewed for sustainability.

Signed

_____

Authorized Signatory

Date:

Appendix 1 – ISMS RACI

Doc Ref Number	Document	Responsible	Accountable	Consult	Inform
IR-0001	Records of training, skills, experience and qualifications (clause 7.2)	HR Manager	HR Manager	Information Security Team	Restricted
IR-0002	Monitoring and measurement results (clause 9.1)	CISO	CISO	Information Security Team	Restricted
IR-0005	Results of the management review (clause 9.3)	CISO	CISO	Heads of Departments	Restricted
IR-0006	Results of corrective actions (clause 10.1)	CISO	CISO	Information Security Team	Restricted
IR-0007	Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)	CISO	CISO	Heads of Functions	All staff
IR-0008	Business impact analysis tool (clause A.17.1.1)	CISO	CISO	Heads of Compliance	All staff
IR-0010	Internal Audit Check List	CISO	CISO	Head of Compliance	Information Security Forum
PR-0001	Change Management Procedure	CIO	CIO	Information Security Forum	All staff
PR-0002	Procedure for Identification of requirement	CISO	CISO	Heads of Functions	All staff

Doc Ref Number	Document	Responsible	Accountable	Consult	Inform
PR-0006	Security Incident management procedure (clause A.16.1.5)	CISO	CIO	Heads Of Functions	All staff
SD-0001	Scope of the ISMS (clause 4.3)	CISO	CISO		All staff
SD-0002	Information security policy and objectives (clauses 5.2 and 6.2)	CISO	CEO		All staff
SD-0003	Risk Management Standard and treatment methodology for Information Security (clause 6.1.2)	CISO	CISO		All staff
SD-0003a	Risk Assessment Table	CISO	CISO		Information Security Team
SD-0003b	Risk Treatment Table	CISO	CISO		Information Security Team
SD-0004	Statement of Applicability (clause 6.1.3 d)	CISO	CISO	Heads Of	Information Security Team
SD-0005	Risk treatment plan (clauses 6.1.3 e and 6.2)	CISO	CISO	Heads Of	Information Security Team
SD-0006	Risk assessment report (clause 8.2)	CISO	CISO	Heads of HR	Information Security Team

Doc Ref Number	Document	Responsible	Accountable	Consult	Inform
SD-0007	Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)	CISO	CISO	Heads of Function	All staff
SD-0008	Inventory of assets (clause A.8.1.1)	CISO	CISO	Head of IT	Restricted
SD-0009	Acceptable use of assets (clause A.8.1.3)	CISO	CISO	Heads of Functions	All staff
SD-0010	Access control policy (clause A.9.1.1)	CISO	CISO	Heads of Functions	All staff
SD-0011	Operating procedures for IT management (clause A.12.1.1)	CISO	CISO	Heads of Functions	All staff
SD-0012	Secure Development Policy (clause A.14.2.1)	CISO	CISO	Engineering Head	Development team
SD-0013	Supplier security policy (clause A.15.1.1)	Head of Procurement	Head of Procurement	CISO	All staff
SD-0014	Incident management Policy (clause A.16.1.5)	Head of Compliance		Information Security Forum	All staff
SD-0015	Business Continuity Plan (clause A.17.1.2)	CISO			All staff

Doc Ref Number	Document	Responsible	Accountable	Consult	Inform
SD-0016	Statutory, regulatory, and contractual requirements (clause A.18.1.1)	CISO	CISO	Information Security Team	All staff
SD-0017	Procedure for document control within the ISMS (clause 7.5)	CISO	CISO	Head of Compliance (Group)	Heads of
SD-0018	Controls for managing records within the ISMS (clause 7.5)	CISO	CISO	Head of Compliance (Group)	Heads of
SD-0019	Procedure for internal audit (clause 9.2)	CISO		Information Security Team	Restricted
SD-0019a	Annual Internal Audit Program	Head of Audit	CISO	Information Security Team	All staff
SD-0019b	Internal Audit Report	Head of Audit	CISO	Heads Of	Information Security Team
SD-0019c	Internal Audit Checklist	Head of Audit	CISO	Heads Of	Information Security Team
SD-0020	Procedure for corrective action (clause 10.1)	CISO	CISO	Heads Of	Information Security Team
SD-0020a	Corrective Action Form	CISO	CISO	Heads Of	All staff
SD-0021	Bring your own device (BYOD) policy (clause A.6.2.1)	CISO		Information Security Team	All staff
SD-0022	Mobile device and teleworking policy (clause A.6.2.1)	CISO		Heads Of	Restricted

Doc Ref Number	Document	Responsible	Accountable	Consult	Inform
SD-0023	Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)	CISO	CISO	Head of Risk and Compliance (Group)	Heads of
SD-0024	Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)	CISO		Heads of	Heads of
SD-0025	Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)	CISO	CISO		All staff
SD-0026	Physical (Office) Security (clause A.11.1.5)	CISO	Head of Facilities	Heads of	All staff
SD-0027	Clear desk and clear screen policy (clause A.11.2.9)	CISO	CISO	Head of	All staff
SD-0028	Change management policy (clauses A.12.1.2 and A.14.2.4)	CISO		Head of Compliance	All staff
SD-0029	Backup policy (clause A.12.3.1)	CISO		Head of Compliance	All staff
SD-0030	Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)	Head of Compliance	Head of Compliance	Head of Compliance	All staff

Doc Ref Number	Document	Responsible	Accountable	Consult	Inform
SD-0031	Business impact analysis (clause A.17.1.1)	CISO	CISO	Heads of	All staff
SD-0032	Exercising and testing plan (clause A.17.1.3)	CISO	Head of Audit		Information Security Forum
SD-0033	Maintenance and review plan (clause A.17.1.3)	CISO	CISO	Information Security Forum	Heads of
SD-0034	Business continuity strategy (clause A.17.2.1)	CISO	CEO	Head of Compliance	Heads of
SD-0035	Data Sharing Agreement	CISO	CISO	Head of Compliance	All staff
SD-0036	Data Protection Policy (clause A.10.1)	CISO	CISO	Head of Compliance	All staff
SD-0037	Health & Safety Policy	Head of HR	Head of HR	Heads of	All staff
SD-0038	Patching Policy	CISO		Information Security Team	All staff
SD-0039	Security Management Team KonaAI and Review AGENDA	Information Security Forum	CISO		All staff
SD-0040	Information and Privacy Policy	CISO	CISO	Head of Compliance	All staff
SD-0041	Management Information Implementation	CISO	CISO		Heads of

Doc Ref Number	Document	Responsible	Accountable	Consult	Inform
SD-0042	Policy for handling classified information	CISO	CISO	Heads of	All staff
SD-0043	ISO27001 & InfoSec Terms & Definitions	CISO	CISO	Information Security Team	All staff

3.0 ORGANIZATION OF INFORMATION SECURITY

3.1 Internal Organization

Reference: ISO/IEC 27002:2013 || A.6.1

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

A management framework shall be established to initiate and control the implementation of information security within the organization. Management shall approve the information security policy, clearly define, and assign security roles, and coordinate and review the implementation of security controls across the organization.

3.1.1 Information security roles and responsibilities || A.6.1.1

All information security responsibilities shall be defined and allocated.

3.1.2 Segregation of duties || A.6.1.2

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

3.1.3 Contact with authorities || A.6.1.3

Appropriated contacts with relevant authorities shall be maintained.

3.1.4 Contact with special interest groups || A.6.1.4

Appropriate contact with relevant authorities shall be maintained.

3.1.5 Information Security in project management || A.6.1.5

Information security shall be addressed in project management, regardless of the type of the project.

3.2 Mobile Devices and Teleworking

Reference: ISO/IEC 27002:2013 || A.6.2

Objective: To ensure the security of teleworking and use of mobile devices.

All mobile devices, including but not limited to, laptops, smart phones are required to be configured to the Information Security Standard to manage risks and ensure appropriate protection is applied. The uses of mobile devices will be governed by KonaAI mobile device policy.

3.2.1 Mobile Device Policy || A.6.2.1

This policy defines standards for connecting to KonaAI networks from any mobile devices. These standards prevent unauthorized access to mobile devices both within and outside of the organization's premises.

Security must be central to an organization's workforce mobility strategy to protect corporate data, maintain compliance, mitigate risks, and ensure mobile security across all devices. With data flowing across public networks, to and from devices that are easily lost or stolen, protecting data becomes a paramount concern and the primary driving force for implementing Mobile Device policy.

KonaAI Mobile Device Policy

- Only devices managed by IT shall be allowed to connect directly to the internal corporate network.
- These devices shall be subject to the valid compliance rules on security features such as encryption, password, key lock, etc.
- All personal mobile computing devices used to access KonaAI-managed data, including but not limited to email, must be passcode-enabled. 2FA shall be enforced by the security team for all employee, contractors.
- Users shall only load corporate data that is essential to their role onto their mobile device(s).
- Users must not load pirated software or illegal content onto their devices.
- Users must report all lost or stolen devices to IT immediately.
- If a user suspects that unauthorized access to KonaAI data has taken place via his/her mobile device, they must report the incident in alignment with KonaAI's incident handling process (Ref: Incident Management Procedure)
- Devices must be encrypted in line with KonaAI's compliance standards.
- These devices should be running the latest version of the operating system available, and all new patches applied.

3.2.2 Teleworking || A.6.2.2

A policy and supporting security measures shall be implemented to protect information accessed, processed, or stored while teleworking.

3.2.3 Kona AI Teleworking Policy

The purpose of this policy is to define requirements for connecting to KonaAI's systems and networks from remote hosts, to minimize data loss/exposure.

- Staff shall be authorized by their Process owners or Head of Department to undertake teleworking. This authorization must be recorded by the HR department.
- This authorization process should involve an assessment of information security risk considering criticality of information assets being accessed; confidentiality of information being handled and suitability of the teleworking technology and location. Final approval must come from the IT department.
- Staff provided with computing and communications equipment for teleworking specifically needs to protect the security of confidential information, must not put the information at risk by using other less secure equipment.
- Teleworking staff must ensure that adequate backup procedures for any information held offsite are implemented. However, it is preferable to remotely access data that is held onsite and already subject to routine backup.
- Access to KonaAI's systems shall be done through an encrypted and authenticated VPN connection with multi-factor authentication enabled.
- Users performing telework shall protect KonaAI's intellectual property rights, either for software or other materials that are present on remote nodes and mobile computing equipment.
- Staff must not permit others to use the equipment provided.
- Staff must not take, send, or print hardcopies of confidential documents offsite.
- Staff must take care of the use of home networks and requirements or restrictions on the configuration of wireless network services, in consultation with IT team.
- IT team must ensure enough Encryption.
- IT team must ensure Anti-virus protection and Firewall.
- IT team must help the staff with methods for securing remote access.
- IT team must have control over equipment and software maintenance.
- IT team must ensure that adequate back-up procedures and business continuity for any information held offsite are properly implemented and maintained.
- IT team must ensure regular Audit and security monitoring.

4.0 HUMAN RESOURCE SECURITY

4.1 Prior to Employment

Reference: ISO/IEC 27002:2013 || A.7.1

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Prior to employment all employees, contractors and third-party users are required to understand their responsibilities, be suitable for the roles they are considered for, and understand their role in safeguarding KonaAI information and information systems.

4.1.1 Screening || A.7.1.1

Background verification checks on all candidates for employment must be carried out in accordance with relevant laws, regulations and ethics and must be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

4.1.2 Terms and Conditions of employment || A.7.1.2

The contractual agreements with employees and contractors must state their own and the organization's responsibilities for information security.

4.2 During the Employment

Reference: ISO/IEC 27002:2013 || A.7.2

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

Upon hire, management will inform each new employee of his/her information security responsibilities and procedures.

4.2.1 Management responsibilities || A.7.2.1

Management must require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

4.2.2 Information Security Awareness, education, and training || A.7.2.1

All employees of the organization and, where relevant, contractors must receive appropriate awareness education and training and regular updates in organization policies and procedures, as relevant for the job function.

(Ref: HR Security Policy)

4.3 Termination & Change of Employment

Reference: ISO/IEC 27002:2013 || A.7.3

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

Managers must ensure that status changes, terminations, and transfers of employees, contractors and third-party users are processed in a timely manner.

4.3.1 Termination or change of employment responsibilities || A.7.3.1

Information Security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced. (Ref: HR Security Policy)

4.4Termination & Change of Employment

Reference: ISO/IEC 27002:2013 || A.7.3

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

Managers must ensure that status changes, terminations, and transfers of employees, contractors and third-party users are processed in a timely manner.

4.4.1 Termination or change of employment responsibilities || A.7.3.1

Information Security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced.

(Ref: HR Security Policy)

5.0 ASSET MANAGEMENT

The purpose of Asset Management Policy is to outline the guidelines and practices that govern decisions on asset management at KonaAI to ensure KonaAI achieves its business objectives.

Asset Management policy applies to all employees and contractors who use Tangible (e.g., laptops, servers) and Intangible information assets (e.g., trademarks, patents) of KonaAI.

5.1 Responsibility for Asset

Reference: ISO/IEC 27002:2013 || A.8.1

Objective: To identify organizational assets and define appropriate protection responsibilities.

All KonaAI assets must be managed as per KonaAI asset management processes and must have a designated Asset Owner. Controls may be delegated by the owner as appropriate to a Process, however the owner remains responsible for the proper protection of the assets.

5.1.1 Inventory of assets || A.8.1.1

Information, other asset associated with the information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

5.1.2 Ownership of assets || A.8.1.2

Assets maintained in the inventory shall be owned.

5.1.3 Acceptable use of Assets || A.8.1.3

Rule for acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented, and implemented.

5.1.4 Return of Assets || A.8.1.4

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

5.2 Information Classification

The purpose of Data Classification Policy is to ensure that information and data is classified appropriately in Vertical and use this classification to build right security and controls to protect the information.

Data Classification policy applies to following:

- All Information systems
- All data stored in KonaAI's information systems

Reference: ISO/IEC 27002:2013|| A.8.2

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

All information possessed by or used by KonaAI will have a designated information owner. Information owners will assign and annually review the appropriate data classification.

5.2.1 Classification of information || A.8.2.1

Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

5.2.2 Labelling of information || A.8.2.2

An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by Kona AI.

All information is labelled with the appropriate classification label whenever it is shared internally or externally. The labelling shall be applied to information and data in:

- Paper documents
- Emails
- Electronic documents
- Application data
- Electronic media

5.2.3 Handling of assets || A.8.2.3

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

(Ref: Information Classification Policy)

5.3 Media Handling

Reference: ISO/IEC 27002:2013 || A.8.3

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

Kona AI must control and physically protect all media to prevent the spread of viruses, unauthorized disclosure, and compromise of sensitive information. Appropriate operating procedures will be established to protect documents, computer media (e.g., backup tapes and disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction. In addition, media will be disposed of securely and safely when no longer required, in accordance with the Kona AI Physical Security Policy.
(Ref: Physical and Environmental Security Policy)

5.3.1 Management of removable media || A.8.3.1

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

5.3.2 Disposal of Media || A.8.3.2

Media shall be disposed of securely when no longer required, using formal procedures.

5.3.3 Physical media transfer || A.8.3.3

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

5.3.4 KonaAI Media Handling Policy

The purpose of this policy is to manage risks posed by removable media from media access, media storage, media transport, and media protection through the establishment of an effective Media Protection Program.

Media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, mobile devices including portable storage media such as USB memory sticks and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, tablets, smartphones and cellular telephones digital cameras, and audio recording devices and non-digital media (e.g., paper, microfilm).

1. KonaAI shall develop Media protection procedures and disseminate within the organization.
2. Media Storage and Access: Access to sensitive media shall be restricted to authorized personnel.

   Based on KonaAI's stance to either restrict access completely or do so in a secure manner. Security controls shall be put in place to protect the confidentiality and integrity of data contained on removable storage media from unauthorized disclosure and modification throughout the life of those storage media, including disposal.
3. Media Marking: All data shall be labelled to reflect its classification. Recipients of information must maintain an assigned label and protect the information.
4. Media Storage: KonaAI shall ensure media is stored in a secure manner and the information is protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
5. Media Transport: KonaAI shall ensure protection when the media is transported outside of controlled areas using define security safeguards and restricting them to authorized personnel only.
6. Cryptographic Protection: KonaAI shall Implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
7. Media Sanitization: KonaAI shall employ sanitization mechanisms commensurate with the security category or classification of the information.

6.0 ACCESS CONTROL

The purpose of Access Management Policy is to define the level of access each user has to information systems and data in Kona AI. This policy document defines the general rules of access for all information systems in the company.

6.1 Business Requirement of Access Control

Reference: ISO/IEC 27002:2013 || A.9.1

Objective: To limit access to information and information processing facilities

Access to KonaAI information, information processing facilities, and business processes is required to be controlled based on business and security requirements.

6.1.1 Access control policy || A.9.1.1

An access control policy shall be established, documented, and reviewed based on business and information security requirements.

6.1.2 Access to network and network services A.9.1.2

Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

6.2 User Access Management

Reference: ISO/IEC 27002:2013 || A.9.2

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services

Information Owners are required to establish appropriate procedures in coordination with Global Information Security to ensure proper access controls are in place to preserve the confidentiality and integrity of all Kona AI systems, networks, applications, databases, data structures, and client data.

6.2.1 User registration and de-registration ||A.9.2.1

A formal user registration and de-registration process shall be implemented to enable assignments of access right.

6.2.2 User Access provisioning ||A.9.2.2

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

6.2.3 Management of privileged access rights ||A.9.2.3

The allocation and user of privileged access rights shall be restricted and controlled. KonaAI shall restrict access to its facilities, information, and systems to meet legal, regulatory and contractual obligations and to demonstrate good practice.

6.2.4 Management of secret authentication information if users ||A.9.2.4

The allocation of secret authentication information shall be controlled through a formal management process.

6.2.5 Review of user access rights ||A.9.2.5

Asset owners shall review user access rights at regular intervals.

6.2.6 Removal or adjustment of access rights ||A.9.2.6

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change.

6.3 User Responsibilities

Reference: ISO/IEC 27002:2013 || A.9.3

Objective: To make users accountable for safeguarding their authentication information.

Users are responsible for maintaining security in the use of passwords, equipment, and any form of access to KonaAI information.

6.3.1 Use of secret authentication information ||A.9.3.1

Users shall be required to follow the organization's practices in the use of secret authentication information.

6.3.2 Kona AI Access Control Policy

This policy establishes the Access Management Policy, for managing risks from user account management, access enforcement, and monitoring, separation of duties, and remote access through the establishment of an Access Control Process. The access control process helps KonaAI implement security best practices about logical security, account management, and remote access.

The scope of this policy applies to all Information Technology (IT) resources owned or operated by KonaAI. Any information not specifically identified as the property of other parties, that is transmitted or stored on KonaAI's IT resources (including e-mail, messages, and files) is the property of KonaAI. All users of KonaAI (employees, contractors, vendors, or others) IT resources are responsible for adhering to this policy.

- All new access or permission change requests require a New Access Request.
- The administrators of each system are responsible for allocating and authorizing user access rights to that system.
- All access requests must be approved by the team member's manager.
- Access to all KonaAI computing resources, including servers, end-user computing devices, network equipment, services, and applications, must be protected by strong authentication. (Wherever possible, use strong password and Multi-factor authentication. Multi-factor authentication for Google, GitHub and AWS accounts is recommended)
- Authenticated sessions must time out after a defined period of inactivity
- Access requests should be submitted when requesting explicit access to private groups, sub-groups, and repositories, to facilitate deprovisioning.
- Requests for access to Infrastructure assets (servers and databases) require a second layer of approval from Infrastructure Management.
- All access requests must be provisioned as approved. An AR that is approved without a role specified should not be provisioned until the role being requested is identified and re-approved.
- Unused accounts, passwords, access keys must be removed within 30 days.
- Administrative permissions should be considered operational in nature. This means that they are granted for the sole purpose of system management, configuration, and support. They should be recognized as privileged accounts and as such, activities must be logged, and the logs protected and regularly reviewed.
- Privileged access must only be gained through a proxy, or equivalent, that supports strong authentication (such as MFA) using a unique individual account with full auditing of user activities.
- Direct administrative access to production systems must be kept to an absolute minimum.
- Time-based access may be provided if administrative action is required for a set period. This should be documented, as part of the Access Request SLAs.
- All requests for new service accounts require a New Service Account Request
- All requests for new service accounts must be approved by a member of Infrastructure Management.
- Access for third party workers, contractors and partners must be enabled for the approved period during which their partner agreement or contract is valid.
- Remote access to third party contractors shall be provided only after a formal request.

6.4 System and Application Control

Reference: ISO/IEC 27002:2013 || A.9.4

Objective: To prevent unauthorized access to systems and applications.

KonaAI systems and applications are required to be configured to prevent unauthorized access to information held in application systems, control user access and protect from malicious software that is capable of overriding or bypassing system or application controls.

6.4.1 Information access restriction || A.9.4.1

Access to information and application system functions shall be restricted in accordance with the access control policy.

6.4.2 Secure log-on procedures || A.9.4.2

Where required by the access control policy access to systems and applications shall be controlled by a secure log-on procedure.

6.4.3 Password Management system || A.9.4.3

Password management system shall be interactive and shall ensure quality passwords.

6.4.4 Use of privileged utility programs || A.9.4.4

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

6.4.5 Access control to program source code || A.9.4.5

Access to program source code shall be restricted.

7.0 CRYPTOGRAPHY

7.1 Cryptographic Control

Reference: ISO/IEC 27002:2013 || A.10.1

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity or information

KonaAI will develop and implement the parameters for use of cryptographic controls including key management.

When encryption is used, government-approved standard algorithms and standard implementation will be employed. Strong encryption algorithms currently accepted in the industry will be used.

7.1.2 Policy on the use of cryptographic controls || A.10.1.1

A policy on the use, protection, and lifetime of cryptographic controls for the protection of information shall be developed and implemented.

7.1.2 Key management A.10.1.2

A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented.

7.1.3 Kona AI Data Encryption Policy

This policy defines organizational requirements for the use of cryptographic controls, as well as the requirements for cryptographic keys, to protect the confidentiality, integrity, authenticity, and nonrepudiation of information at KonaAI.

This policy covers encryption for the following:

- Laptop, tablet computers, mobile phones and PDAs, Desktops, servers, etc.
- USB memory sticks, external hard drives, DVDs/CDs, backup tapes
- E-mail
- Applications

The policy is applicable to all KonaAI employees that consume/process information through an electronic medium.

1. Kona AI IT team shall create an inventory of the endpoints in the network to get a complete picture of the device types, operating systems, and supported encryption methods.
2. KonaAI shall employ a high level of protection of the confidentiality of encryption keys throughout their whole lifecycle. All cryptographic keys should be protected against modification, loss, and destruction and confidential keys need protection against unauthorized disclosure.
3. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise. They need to be vaulted in a hardware security module (HSM), which provides hardware-based protection.
4. KonaAI shall ensure Encryption of data in transition and rest by employing best practices for the same.

8.0 PHYSICAL AND ENVIRONMENTAL SECURITY

The Information Security Policy is designed to work in partnership with the Physical and Environmental Security Policy written and maintained by the Chief Physical Security Office. Please refer to the Physical and Environmental Security Policy.

8.1 Secure Areas

Reference: ISO/IEC 27002:2013 || A.11.1

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information or information processing facilities.

8.1.1 Physical security perimeter || A.11.1.1

Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

8.1.2 Physical entry controls || A.11.1.2

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

8.1.3 Secure offices, rooms, and facilities || A.11.1.3

Physical security for offices, rooms and facilities shall be designed and applied.

8.1.4 Protecting against external and environmental threats || A.11.1.4

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

8.1.5 Working in secure areas || A.11.1.5

Procedures for working in secure areas shall be designed and applied.

8.1.6 Delivery and loading areas || A.11.1.6.

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access

(Ref: Physical and Environmental Security Policy)

8.2 Equipment

Reference: ISO/IEC 27002:2013 || A.11.2

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

Equipment shall be sited and protected to reduce the risk from environmental threats and hazards, and opportunities for unauthorized access.

8.2.1 Equipment siting and protection ||A.11.2.1

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

8.2.2 Supporting Utilities ||A.11.2.2

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

8.2.3 Cabling Security ||A.11.2.3

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage.

8.2.4 Equipment Maintenance ||A.11.2.4

Equipment shall be correctly maintained to ensure its continued availability and integrity.

8.2.5 Removal of Assets ||A.11.2.5

Equipment, information, or software shall not be taken off-site without prior authorization.

8.2.6 Security of equipment and assets off-premises ||A.11.2.6

Security shall be applied to off-site assets considering the different risks of working outside the organization's premises.

8.2.7 Secure disposal or re-use of equipment ||A.11.2.7

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

8.2.8 Unattended user equipment ||A.11.2.8

Users shall ensure that unattended equipment has appropriate protection.

8.2.9 Clear desk and clear screen policy ||A.11.2.9

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

(Ref: Physical and Environmental Security Policy)

9.0 OPERATIONS SECURITY

9.1 Operational Procedures and Responsibilities

Reference: ISO/IEC 27002:2013 || A.12.1

Objective: To ensure correct and secure operations of information processing facilities.

9.1.1 Documented operating procedures || A.12.1.1

Operating procedures shall be documented and made available to all users who need them.

9.1.2 Change Management || A.12.1.2

Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

(Ref: Change Management Procedure)

9.1.3 Capacity Management || A.12.1.3

The use of resources shall be monitored, tuned and projections made of future capacity requirement to ensure the required system performance.

To limit disruption to the network, applications, and business functions, KonaAI will monitor system capacity and plan for future capacity needs in sufficient time to procure system resources prudently. This will ensure adequate resources are available and reduce the possibility of system overload.

System owners shall monitor their equipment for current uses and projected capacity.

IT Capacity Management shall ensure:

- Availability and integrity of the information technology infrastructure
- Capacity of information technology resources meet current and future business needs
- Availability and performance of information resources are maintained at agreed service levels
- The utilization or performance of the resources are measured
- Workload forecasts are transformed into IT resource requirements
- Requirements are mapped onto existing utilization
- Monitoring of performance and throughput of IT Services and the supporting Infrastructure components.
- Optimization and changes are performed
- The organization shall demonstrate that the use of resources is monitored, tuned up, and that projections of future capacity requirements are made.
- Periodic reports of capacity performance, breaches in SLA's, cost vs. budgets, resource forecasts are prepared for management review by the Capacity Manager.

9.1.4 Separation of development, testing and operational environments || A.12.1.4

Development, testing and operational environment shall be separated to reduce the risks of unauthorized access or any negative impact on the operational environment.

9.2 Protection for Malware

To establish requirements which must be met by all computers (laptops, desktop, mobile devices) and servers connected to Kona AI network to ensure effective virus detection and prevention.

Reference: ISO/IEC 27002:2013 || A.12.2

Objective: To ensure that information and information processing facilities are against malware.

9.2.1 Control against Malware || A.12.2.1

KonaAI will protect networks and systems from malicious damage by implementing controls to detect, prevent and recover from malicious code. All software applications are required to be kept up-to-date and free of viruses. Appropriate user awareness procedures will be implemented. When software applications are no longer supported by the manufacturer, and security patches or updates are no longer produced, the software applications are required to be upgraded to a supported version, or a business justification and risk review will be completed and documented with approval of the business sponsor and the Information Security Office.

9.3 Backup

Reference: ISO/IEC 27002:2013 || A.12.3

Objective: To protect against loss of data.

9.3.1 Information backup || A.12.3.1

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

Information Owners are responsible for ensuring that backup operations and procedures for recovery are in place and meet the needs of the Process they support.

The designated Process will afford backup files the same degree of security and protection as the original data and ensure archived storage media is appropriate for required longevity and format.

9.4 Logging and Monitoring

Reference: ISO/IEC 27002:2013 || A.12.4

Objective: To record events and generate evidence.

Event logs shall be enabled to record user activities, exceptions, and information security events shall be produced, kept, and regularly reviewed.

Information Owners or their designees will ensure that the systems are configured to deliver audit trails where applicable as per the classification of the data and its control requirements. The audit data will show how information in the systems arrived at its present state and who was responsible for the last change made to the data.

9.4.1 Event logging ||A.12.4.1

Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept and regularly reviewed.

9.4.2 Protection of log information ||A.12.4.2

Logging facilities and log information shall be protected against tampering and unauthorized access.

9.4.3 Administrator and operator logs ||A.12.4.3

System administrator and system operator activities shall be logged, and the logs protected and regularly reviewed.

9.4.4 Clock synchronization ||A.12.4.4

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.

9.4.5 Kona AI Logging and Monitoring Policy

The purpose of this policy is to provide accurate and comprehensive audit logs across KonaAI environment to provide key information, detect and detect indicators of potential compromise.

This policy applies to all Information Systems that store, process, or transmit KonaAI Data.

1. All production systems within KonaAI shall record and retain audit-logging information.
2. Information System audit logs must be protected from unauthorized access or modification.
3. Information System audit logs must be retained for an appropriate period, based on the Document Retention Schedule and business requirements. Audit logs that have exceeded this retention period should be destroyed according to KonaAI Data disposal policy.
4. Unless technically impractical or infeasible, all logs must be aggregated in a central system so that activities across different systems can be correlated, analyzed, and tracked for similarities, trends, and cascading effects.
5. Logs shall be reviewed on a regular basis.

9.5 Control of Operational Software

Reference: ISO/IEC 27002:2013 || A.12.5

Objective: To ensure the integrity of operational systems

9.5.1 Installation of software on operational systems ||A.12.5.1

Procedures shall be implemented to control the installation of software on operational systems.

9.6 Vulnerability Management

Reference: ISO/IEC 27002:2013 || A12.6

Objective: To prevent exploitation of technical vulnerabilities.

Technical Vulnerabilities of information systems are required to be identified, evaluated, managed, and mitigated in an effective and timely manner.

9.6.1 Management of technical vulnerabilities || A.12.6.1

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

9.6.2 Restriction of software installation

Rules governing the installation of software by users shall be established and implemented.

9.7 Information Systems Audit Considerations

Reference: ISO/IEC 27002:2013 || A.12.7

Objective: To minimize the impact of audit activities on operational systems.

Kona AI is required to take precautions to ensure internal and external audits, when conducted, minimize the amount of interference to information systems and business processes.

9.7.1 Information systems audit controls

Audit requirements and activities involving verification of operational systems shall be carefully and agreed to minimize disruptions to business processes.

10.0 COMMUNICATIONS SECURITY

10.1 Network Security Management

Reference: ISO/IEC 27002:2013 || A.13.1

Objective: To ensure the protection of information in networks and its supporting information processing facilities

Networks shall be adequately segregated, managed, and controlled with security mechanisms and service levels to be included in network service agreement, to be protected from threats, and to maintain security for the systems and applications using the network.

10.1.1 Network controls || A.13.1.1

Networks shall be managed and controlled to protect information in systems and applications.

10.1.2 Security of network services || A.13.1.2

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

10.1.3 Segregation in networks || A.13.1.3

Groups of information services, users and information systems shall be segregated on networks.

10.2 Information Transfer

Reference: ISO/IEC 27002:2013 || A.13.2

Objective: To maintain the security of information transferred within an organization and with any external entity

Data transfer agreements, procedures, controls, agreement for secure transfer between KonaAI and external parties, shall be in place to protect the transfer of information through all types of communication.

10.2.1 Information transfer policies and procedures ||A.13.2.1

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information using all types of communication facilities.

10.2.2 Agreements on information transfer ||A.13.2.2

Agreements shall address the secure transfer of business information between the organization and external parties.

10.2.3 Electronic messaging ||A.13.2.3

Information involved in electronic messaging shall be appropriately protected.

10.2.4 Confidentiality or non-disclosure agreements ||A.13.2.4

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.

11.0 SYSTEM ACQUISITION DEVELOPMENT AND MAINTENANCE

Prior to the development and/or implementation of information systems, security requirements are required to be identified and agreed upon in coordination with the Kona AI Security Office.

11.1 System Requirements of Information Systems

Reference: ISO/IEC 27002:2013 || A.14.1

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

Prior to the development and/or implementation of information systems, security requirements are required to be identified and agreed upon in coordination with the KonaAI Information Security team.

11.1.1 Information security requirement analysis and specification || A.14.1.1

The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

11.1.2 Securing application services on public networks || A.14.1.2

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

11.1.3 Protecting application services transactions || A.14.1.3

Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alternation, unauthorized disclosure, unauthorized message duplication or replay.

11.2 Security in Development and Support Processes

Reference: ISO/IEC 27002:2013 || A.14.2

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

Information Owners and Application Owners are responsible for the security of the project or support environment. They are required to ensure all proposed system changes are reviewed and do not compromise the security of the system or the operating environment.

The Kona AI Information Security team is responsible for promulgating approved KonaAI secure coding standards for use in each phase of the software development life cycle. Managers are responsible for ensuring that procedures used in the software development lifecycle conform to Kona AI Security requirements and approved KonaAI secure coding standards and will be held accountable for adherence to these standards.

11.2.1 Secure development policy || A.14.2.1

Rules for the development of software and systems shall be established and applied to developments within KonaAI. (Ref: Secure Software Development Lifecycle Policy)

11.2.2 Systems change control procedure || A.14.2.2

Changes to systems within the developments lifecycle shall be controlled using formal change control procedures.

(Ref: Change Control Procedure, Secure Software Development Lifecycle Procedure)

11.2.3 Technical review of applications after operating platform changes || A.14.2.3

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

11.2.4 Restrictions on changes to software packages || A.14.2.4

Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

11.2.5 Secure systems engineering principles || A.14.2.5

Principles for engineering secure systems shall be established, documented, maintained, and applied to any information systems implementation efforts.

11.2.6 Secure development environment || A.14.2.6

KonaAI shall establish and appropriately protect secure development environments for system development and integration efforts that covers the entire system development lifecycle.

11.2.7 Outsourced development || A.14.2.7

KonaAI shall supervise and monitor the activity of outsourced system development.

11.2.8 System security testing || A.14.2.8

Testing of security functionality shall be carried out during development.

11.2.9 System acceptance testing || A.14.2.9

Acceptance testing programs and related criteria shall be established for new information systems, upgrades, and new version.

Related Document:

(Ref: Secure Software Development Lifecycle Policy and Procedure)

11.3 Test Data

Reference: ISO/IEC 27002:2013 || A.14.3

Objective: To ensure protection of data used for testing

11.3.1 Protection of test data || A.14.3.1

Test data shall be selected carefully, protected, and controlled.

12.0 SUPPLIER RELATIONSHIPS

12.1 Information Security in Supplier Relationships

Reference: ISO/IEC 27002:2013 || A.15.1

Objective: To ensure protection of the organization's assets that is accessible by suppliers

12.1.1 Information security policy for supplier relationships || A.15.1.1

Information security requirements for mitigating the risks associated with supplier's access to the KonaAI assets shall be agreed with the supplier and documented.

12.1.2 Addressing security within supplier agreements || A.15.1.2

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, KonaAI information.

12.1.3 Information and communication technology supply chain || A.15.1.3

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

12.1.4 KonaAI Vendor Management Policy

This policy defines the rules for relationships with the organization's Information Technology (IT) vendors and partners. It applies to all contractors, service providers and vendors of KonaAI.

1. Vendor on boarding: KonaAI shall perform due diligence review in selecting a vendor, analysing risks, monitoring and other areas of third-party risk management.
2. IT vendors shall be prohibited from accessing KonaAI's information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.
3. All IT vendors must comply with the security policies defined and derived from the Information Security Policy.
4. Ensure vendor must meet a certain level of security- SOC2 security requirements. Obtain all regulatory compliance reports. Check if they do annual penetration tests.
5. A Statement of Work (SOW) clearly stating the security requirements for the vendors to ensure that their work is consistent with KonaAI's cyber security requirements. SOW must clearly identify all types of sensitive data to be exchanged and managed by the vendor. Sensitive data is defined as either regulated or confidential by the (Ref: Data Classification Policy)
6. Contracts for software and other services delivered from cloud vendors shall be reviewed by the Information Security Officer for security compliance. The service-level agreements should have a crystal-clear understanding of their responsibilities.
7. KonaAI shall Establish Service level agreements (SLAs) standards and monitor performance of vendors against these.
8. Contracts that include exchange of sensitive data must require confidentiality agreements to be executed by the vendor, must identify applicable KonaAI policies and procedures to which the vendor is subjected, and must identify security incident reporting requirements.
9. Contracts must clearly identify security reporting requirements that stipulate that the vendor is responsible for maintaining the security of sensitive data, regardless of ownership. In event of a breach of the security of the sensitive data, the vendor is responsible for immediately notifying KonaAI IT team and work with them for both recovery and remediation.
10. KonaAI shall ensure that key risks are identified and monitored.
11. IT vendors and partners must ensure that KonaAI's records are protected, safeguarded, and disposed of securely. They shall strictly adhere to all applicable legal, regulatory, and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally Identifiable Information (PII).

12. The vendor shall be responsible for notifying all persons whose sensitive data may have been compromised, because of the breach as required by law.
13. Ongoing oversight review shall include technical vulnerabilities testing, annual site visit and an inspection of documentation, such as security test results and disaster recovery plans.
14. KonaAI may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory, and contractual obligations.
15. Upon termination of vendor services, contracts must require the return or destruction of all KonaAI data in accordance with Access Control Policy. Procurement managers are to immediately ensure termination of all access to KonaAI information systems and, if applicable, facilities housing these systems.
16. KonaAI shall establish redundancies whenever possible- create an internal response plan for each vendor in the event of a failure.
17. KonaAI shall hold vendors to the same standards (specific security expectations). They are to be included in the vendor contract details up front.
18. Through policy, standards, guidelines, and procedures, the vendor management program shall formally address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance requirements.

12.2 Supplier Service Delivery Management

Reference: ISO/IEC 27002:2013 || A.15.2

Objective: To maintain an agreed level or information security and service delivery in line with supplier agreements

12.2.1 Monitoring and review of supplier services || A.15.2.1

KonaAI shall regularly monitor, review and audit supplier service delivery.

12.2.2 Managing changes to supplier services || A.15.2.2

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

13 INFORMATION SECURITY INCIDENT MANAGEMENT

13.1 Management of Information Security Incidents & Improvements

The purpose of Incident Management Policy is to outline the procedures in place at Kona AI to monitor, alert, respond and mitigate security incidents.

Reference: ISO/IEC 27002:2013 || A.16.1

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Kona AI will manage each security incident, to mitigate any damage in a consistent and effective manner. Potential information security incidents include but are not limited to unauthorized use of computers and other information systems, unauthorized exposure or alteration of confidential data, loss of the normal ability to access information, and virus attacks.

13.1.1 Responsibilities and procedures || A.16.1.1

Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.

13.1.2 Reporting Information security events || A.16.1.2

Suspected information security incidents and security weaknesses will be reported immediately to the KonaAI Information Security team.

Formal security event reporting channels and escalation procedures shall be in place to ensure corrective action occurs in a timely manner.

13.1.3 Reporting Information security weakness || A.16.1.3

KonaAI employees and contractors using KonaAI information system and services shall require noting and reporting any observed or suspected information security weakness in systems or services.

13.1.4 Assessment of and decision on information security events || A.16.1.4

Information security incidents shall be assessed, and it shall be decided if they are to be classified as information security incidents.

13.1.5 Response to information security incidents || A.16.1.5

KonaAI will manage each security incident to mitigate any damage in a consistent and effective manner.

When an incident is reported, the KonaAI Security group will collaborate with other teams to investigate and respond to the incident in accordance with the documented procedures.

13.1.6 Learning from information security incidents || A.16.1.6

The information gained from assessment and resolving information security incidents shall be used to improve operations and reduce the likelihood or impact of future incidents.

13.1.7 Collection of evidence || A.16.1.7

Kona AI shall define and apply procedures for the identification, collection, acquisition, and preservation of information which can serve as evidence conforming to the rules for evidence in relevant jurisdiction(s).

(Ref: Incident Management Policy and Procedure)

14 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

The Information Security Policy is designed to work in partnership with the Business Continuity Policy and Standard. (ref Business Continuity Policy)

14.1 Information Security Continuity

The purpose of this policy is to outline objectives, plans and, procedures put in place by KonaAI to ensure that it minimizes disruption to the organization's key business activities caused by a major security incident or a natural disaster.

Reference: ISO/IEC 27002:2013 || A.17.1

Objective: Information security continuity shall be embedded in the organization's business continuity management systems.

KonaAI will counteract all interruptions to business activities and protect critical business processes from the effects of major failures of information systems or disasters. Timely resumption will be ensured.

14.1.1 Planning information security continuity || A.17.1.1

KonaAI will determine its requirement for information security and its continuity in adverse situations, e.g., during a crisis or disaster.

14.1.2 Implementing information security continuity || A.17.1.2

KonaAI shall establish, document, implement and maintain processes, procedures, and controls to ensure the required level of information security is maintained during an adverse situation.

14.1.3 Verify, review and evaluate information security continuity || A.17.1.3

KonaAI shall verify the implemented security continuity controls at regular intervals to ensure they are effective and valid during adverse situations.

(Ref: Business Continuity Policy)

14.2 Redundancies

Reference: ISO/IEC 27002:2013 || A.17.2

Objective: To ensure availability of information processing facilities

14.2.1 Availability of information processing facilities || A.17.2.1

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements of KonaAI business.

15.0 COMPLIANCE

15.1 Compliance With Legal and Contractual Requirements

Reference: ISO/IEC 27002:2013 || A.18.1

Objective: To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements

KonaAI will comply with applicable laws, statutory, regulatory, or contractual obligations, and any applicable security requirements to reduce KonaAI's exposure to security threats.

15.1.1 Identification of applicable legislation and contractual requirements || A.18.1.1

All relevant legislative statutory, regulatory, contractual requirements and KonaAI approach to meet these requirements shall be explicitly identified, documented, and kept up to date for each information system and the organization.

15.1.2 Intellectual property rights || A.18.1.2

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.

15.1.3 Protection of records || A.18.1.3

Records shall be protected from loss, destruction, falsification, unauthorized access and authorized access and unauthorized release, in accordance with legislator, regulatory, contractual, and business requirements.

15.1.4 Privacy and protection of personally identifiable information || A.18.1.4

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

15.1.5 Regulation of cryptographic controls || A.18.1.5

Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

15.2 Information Security Reviews

Reference: ISO/IEC 27002:2013 || A.18.2

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures

KonaAI is required to take precautions to ensure internal and external audits, when conducted, minimize the amount of interference to information systems and business processes.

15.2.1 Independent review of information security || A.18.2.1

KonaAI information security implementation shall be reviewed independently at planned intervals or when significant changes occur.

15.2.2 Compliance with security policies and standards || A.18.2.2

Information Security Manager/CISO shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

15.2.3 Technical compliance review || A.18.2.3

Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

16.0 CLOUD SECURITY

16.1 Governance and Compliance

Cloud services must be approved prior to deployment by Global Information Security. Security assurance services must be performed on KonaAI hosted environment and necessary evidence to be acquired to evaluate the security posture of the environment.

16.2 Identity and Access Management

Access to the cloud service providers must be strictly controlled to ensure only those with a required need to access such services are permitted and have the appropriate level of access.

16.3 Cryptography and Key Management

Policies and procedures shall be established for the management of cryptographic keys which should include but not limited to the lifecycle management from key generation, revocation, replacement, exchange, and storage.

16.4 Data Protection

Data must be adequately protected whilst being processed, in transit and at rest to protect against threat to its confidentiality, availability and integrity in line with the data classification and its intended use.

16.5 Infrastructure and Application Security

Infrastructure, application, and APIs should be designed, developed, deployed and tested in accordance with leading industry standards and must adhere to applicable legal and regulatory compliance.

16.6 Segregation and Virtualization

KonaAI hosted environment must be segregated from other tenant hosted environments in an appropriate manner to support the necessary services and security requirement of the business.

16.7 Logging, MONITORING, and Incident Response

KonaAI hosted environment must be monitored from a security perspective to capture events of interest and provide overall visibility of the cloud service security posture.

KonaAI security response process must be integrated with cloud service solution to ensure incidents can be responded to in a timely manner and where necessary evidence can be acquired to support investigations.

17.0 INFORMATION SECURITY POLICY:

17.1 Managing Information Security

Objective: KonaAI's main objectives for information security include the following:

- **17.1.1** The organization's objectives for information security are in line with the organization's business objectives, strategy, and plans.
- **17.1.2** Objectives for individual security controls or groups of controls are proposed by KonaAI management team, including but not limited to Chief Information Security Officer (CISO) and others as appointed by the CEO; these security controls are approved by the CEO in accordance with the Risk Assessment Policy (Reference: Risk Assessment Policy)
- **17.1.3** All objectives shall be reviewed at least once per year.
- **17.1.4** KonaAI will measure the fulfilment of all objectives. The measurement will be performed at least once per year. The results must be analysed, evaluated, and reported to the management team.
- **17.1.5** Information Security Requirements
- **17.1.6** This policy and the entire information security program must be compliant with legal and regulatory requirements as well as with contractual obligations relevant to KonaAI.
- **17.1.7** All employees, contractors, and other individuals subject to the organization's information security policy must read and acknowledge all information security policies.
- **17.1.8** The process of selecting information security controls and safeguards for the organization is defined.
- **17.1.9** Security requirements for the software development life cycle, including system development, acquisition and maintenance are defined in the Secure Software Development Lifecycle Policy (Reference: SSDLC Policy)
- **17.1.10** Security requirements for handling information security incidents are defined in the Security Incident Response Policy (Reference: Incident Management Policy).
- **17.1.11** Disaster recovery and business continuity management policy is defined in the Business Continuity Policy (Reference: Business Continuity Policy).

18.0 COMPLIANCE

Compliance with this policy and any supporting policies, standards and processes is essential to reduce Kona AI's exposure to security threats.

Kona AI to exercise due care for the safeguarding of data in custody, but not limited to, Personally Identifiable Information (PII), Protected Health Information (PHI) and KonaAI Intellectual Property. An independent review of compliance with this policy shall be conducted on a regular basis.

The Chief Information Security Officer shall ensure compliance.

Any person, subject to this policy, who fails to comply shall be subjected to appropriate disciplinary action in accordance with the Kona AI Disciplinary Code and Procedures.

19.0 EXCEPTIONS

Any exceptions to the policy shall be carried out as per the (Ref: Exceptions Policy)

20.0 REVIEW AND UPDATE FREQUENCY

The policy will be reviewed annually and/or when significant changes occur.

Changes of this policy shall be exclusively performed by the CISO and approved by the Management.

A Change log shall be kept current and be updated as soon as any change has been made.

20.1 Documented Operating Procedures

The process and procedures supporting these policy requirements shall be documented, maintained, and made available to all users who need them.

21.1 RELATED POLICIES

The following are all relevant policies and procedures to this policy:

- Acceptable Use Policy
- Mobile Device Policy
- Teleworking Policy
- Access Control Policy
- Data Encryption Policy
- Physical and Environmental Security
- Logging and Monitoring Policy
- HR Security Policy
- Risk Assessment Policy
- Data Classification Policy
- Incident Response Policy
- Business Continuity Policy

konaAI

Contact Us

https://konaai.com/

https://www.linkedin.com/in/kona-ai/

https://twitter.com/kona__ai

info@konaai.com