CYBERSECURITY POLICY

KIRON CAPITAL GESTÃO DE RECURSOS LTDA

Version 1.2
August 2021

1 OBJECT

This Policy aims to define KIRON's principles and metrics that will guide the assessment of information security risks, control and prevention of attacks, appropriate response to incidents, as well as the awareness by all KIRON partners, members, officers, employees (permanent or temporary) and trainees (collectively, "Collaborators") regarding the importance of adopting security practices.

Through this policy, we seek to control, monitor and protect the following:

(i) KIRON's customer base (current and potential);
(ii) Database (including historical information) used by the company;
(iii) KIRON's business plan and its investment strategies;
(iv) Intellectual Property, such as modeling methodologies that are developed by KIRON Collaborators;
(v) Lists of users and passwords; and
(vi) Access to sensitive files and folders, as well as asset trading systems used by KIRON.

1.1 Concepts and definitions

The following are all the technical terms used in preparing this Policy:

- Backup: copies of data made in order to protect that data against possible failures or losses;
- ISC – Information Security Committee: group of collaborators designated to handle specific Information Security issues;
- CSIRT – Computer Security Incident Response Team: technical group responsible for handling and responding to Information Security Incidents;
- Login: process of accessing a restricted computer system. Usually this process requires a process of authentication and authorization;
- Logs: records of events observed in certain computerized systems (for example: an attempt to access a system will generate a log of this action).
- Passphrase: a type of password that, instead of being based on a word, uses whole sentences to increase the complexity and security of the password;
- Restore: act of retrieving data from a backup copy;
- SMS – Short Message Service: a digital cellular phone service for sending short text messages;
- SNMP – Simple Network Management Protocol: type of protocol for managing and monitoring network devices;
- SPAM: term used to characterize unwanted messages that are normally sent in an automated way to several different users;
- Token: device that can be electronic (physical) or virtual (app) that generates single-use passwords to be used in conjunction with the personal passwords of each user;
- Network User: any individual or institution that has authenticated access to KIRON corporate network resources;
- System User: any individual or institution that has authenticated access to the systems made available by KIRON;
- VPN – Virtual Private Network: a private communications network built on a public communications network (such as the Internet);

This Policy should be read in conjunction with the KIRON Compliance Manual ("Manual"). Defined terms, if not referred to herein, shall have the meanings assigned to them in the Manual.

2 Principles

KIRON is aware that investment managers cannot ignore cybersecurity risks. Information security is an ever-increasing demand not only by regulators but customers and partners as well, so proactive action in cybersecurity risk management is a crucial tool for ensuring confidentiality, integrity, and availability of KIRON's data and systems and those of its clients.

KIRON adopts the following principles to ensure the successful implementation of this Information Security Policy in the company:

- KIRON's Executive Board should actively support the Information Security and Internal Communication actions, in order to demonstrate to other Collaborators the commitment necessary to achieve the defined goals and targets;
- Access to information and corporate computing resources should be released only after the Collaborator has reviewed and declared to be aware of his/her responsibilities regarding compliance with the guidelines of this Information Security Policy;
- In cases where there is a violation, non-compliance or risk of an Information Security breach, the KIRON Information Security Committee (ISC) shall be immediately notified in order to initiate actions to respond to the incident in question;
- Any omissions in this standard should be resolved by the ISC with the support of the Chief Compliance Officer or the Executive Board.

2.1 Information Security Committee

The Information Security Committee (ISC) is composed of KIRON Collaborators and the Chief Compliance Officer, the purpose of which is to strengthen information security processes and culture, in addition to the following roles and responsibilities:

- Assist/advise in the implementation of the company's information security actions;
- Request and monitor or conduct investigations and evaluations to identify whether the current policy is appropriate to the company's needs and is being followed properly;
- In the event of a security incident, deploy the third-party Computer Security Incident Response Team

3 Guidelines and Procedures for fulfillment

The following are the minimum guidelines that should be followed for each topic, considering the best practices and specific Security standards:

3.1 Information treatment

All information provided by KIRON to its Collaborators should be treated in a restricted manner, and it is prohibited for any such information to be made available to the public, unless approved by the Executive Board or by the Compliance Committee.

Collaborators must also observe the restrictions applicable to the handling of Confidential Information or KIRON Products, as defined in the KIRON Compliance Manual.

3.2 Treatment of Incidents

In the event of a possible incident, the ISC should be immediately notified by the person responsible for identifying the incident, in order for the ISC to be able to deploy the third-party CSIRT (Computer Security Incident Response Team).

The CSIRT is responsible for receiving, analyzing and responding to notifications and activities related to security incidents in KIRON's computer network, as well as collecting and attaching all evidence necessary for the solution or prevention of incidents;

The incident response process performed by the CSIRT should be constantly monitored and documented by KIRON's ISC in order to assess the services performed and to absorb the lessons learned from each situation.

3.3 Access Controls

The rules for accessing the corporate network are:

- Local or remote logical accesses to the KIRON Corporate Network must be carried out only for the specific interests of the company's business;
- Access to the Corporate Network should be done through different access profiles, specific to each Collaborator or user; it is the responsibility of the Executive Board to define the roles, responsibilities and updates of the profiles in question;
- Each profile will have its roles and responsibilities that will grant access to the different technological resources of the corporate network, as defined by the Executive Board;
- The networks and resources destined to company visitors should be used only by its target public;
- The authentication and authorization techniques employed to validate the identity of users on the network are User Name and Personal Password. In cases of remote access to the Corporate Network, a second authentication factor will be mandatory, which must be presented at the time of authentication jointly with the personal password;
- Accesses to systems that require authentication and authorization should always be terminated when completed, or temporarily blocked during interruptions in the service or in the absence of the collaborators responsible;

3.4 Internet access and use of Corporate Email

- The validity of the access to the corporate email account must be bound to the period stipulated in the agreement signed between the user and KIRON;
- Access to the Internet and the corporate email account made available to users of KIRON's network (Wi-Fi and cabled) are for personal and non-transferable use, and each email account holder is solely and fully responsible for the actions and possible damages caused to the Company or to third parties through its use;
- Use of the Internet and corporate email is a concession of KIRON, not a right of the network user, and will be canceled upon termination of the collaborator or at the end of the term of the contract signed with the collaborator;
- It is strictly forbidden the use of the services granted by KIRON to access, receive, store or send malware, pornography, offenses, criminal or unlawful activity, actions that incite violence or that violate copyrights, actions for commercial objectives or that contribute to the continuation of electronic chain messages and SPAM;
- Internet access and corporate email may be monitored and restricted by KIRON at any time;
- All users must submit to the controls implemented in corporate networks, in such a way that the use of systems that provide ways to circumvent these controls is considered a serious violation of this Policy;
- In cases of suspected breach of the General Guidelines of the Information Security Policy, KIRON may access the corporate mailbox of the user of the network in question, as well as request a report with detailed information of the websites accessed and all actions taken by said user while using corporate services.

3.5 Protection and use of passwords

All user and system passwords must follow the guidelines below:

- At least 12 alphanumeric characters;
- Uppercase and lowercase characters;
- At least one numeral;
- At least one special character;
- Whenever possible, it should be based on phrases (passphrases);
- Should not be based on known words;
- Should not contain personal information such as birthday, names, etc.;

- Should not contain corporate information such as names, addresses, systems, functions, etc.;
- Should not be based on patterns or sequences of any kind;
- User accounts that have access privileges to systems through the group hierarchy (Directory Service) or specific programs (for example: SUDO) must use passwords different from all other accounts that the user has for accessing the systems;

Users should not use their corporate passwords in external accounts that are not related to KIRON (for example: social media, personal email, etc.). Whenever possible, avoid using repeated passwords in different corporate systems. All user passwords (for example, email, web, Windows, etc.) should be changed at least once every 12 months.

The CSIRT team may periodically or randomly attempt to crack and guess passwords. If a password is discovered or cracked during these attempts, the user will be prompted to change the password to a new one that complies with the guidelines in this document.

4 Risk management

Risk management should use the following as analytical objects: (i) Management Activities and Company Activities (as defined in the KIRON Code of Ethics); (ii) physical facilities and their surroundings where the critical activities are found; (iii) the necessary Information Technology infrastructure; and (iv) the human resources that support these activities.

As procedures for cybersecurity risk management, KIRON adopts two complementary approaches, shown below:

4.1.1 Continuity Management

KIRON shall adopt the following practices to ensure continuity and cybersecurity:

- Use a backup and restore mechanism for all services and products developed by KIRON as well as its database;
- Ensure that all information technology resources, when compatible, are properly configured to maintain logs of all security-relevant events (logins, access attempts, changes in general, etc.);
- Review, update and test the cybersecurity measures implemented on an annual basis, or whenever there are significant changes in activities that support KIRON products and services.
- Ensure that the development of new products, services and business inherent in KIRON operations is done in a way that complies with this Cybersecurity Policy, as well as ensuring that changes to existing products and services are in line with security, quality, efficiency and operational continuity;
- Immediately report any incidents that present a continuity risk to the responsible areas (ISC and CSIRT), in order to allow immediate action to be taken by deploying the respective continuity or recovery plans;
- Document the impact of any possible interruption of activities that support KIRON's critical products and services under the terms of the KIRON Contingency Plan;
- Identify tactical solutions that support the restoration of the required activities within the desired recovery time, in case of possible unavailability;
- Establish an efficient, independent and full-time communication channel for service and guidance in the event of incidents that could jeopardize the security of KIRON's assets or information.

4.1.2 Audit and Compliance

KIRON's policy is to carry out independent inspections, conducted by an auditor at least once every two years, with the aim of testing the adequacy of information technology resources, in order to: (i) ensure compliance with the Security Policy Guidelines and Procedures. Information; and (ii) update and recommend any changes to the controls, policies and procedures adopted.

The audit records must be stored at KIRON headquarters for a period of no less than two years.

5 Penalties

In the event of non-compliance or violation of the guidelines pertaining to this Policy, KIRON may apply sanctions and other measures that the Executive Board deems necessary, such as: immediate dismissal for just cause, reimbursement of financial losses, legal remedies for moral damages, etc.

6 Periodic Reviews

The KIRON Information Security Policy must always be up-to-date and in line with the interests and needs of the company. The ISC, jointly with the Chief Compliance Officer, shall review the Cybersecurity Policy at least annually. Whenever any change is made, approved and enters into force, such change shall be widely disseminated so that all Collaborators have the opportunity to review and certify their awareness about the new rules implemented or those that have been updated.