SCICROP® INFORMATION SECURITY POLICY

Last update:	(English translation) 25/07/2022
Version.Revision:	1.4
Author	José Damico <damico@scicrop.com>

1. INTRODUCTION

a. The Information Security Policy, hereinafter referred to as ISP-SciCrop, is the document that guides and establishes SciCrop's corporate guidelines for the protection of information assets and prevention of legal liability for all users. It must, therefore, be complied with and applied in all areas of the institution.

b. This ISP-SciCrop is based on the recommendations proposed by ABNT NBR ISO/IEC 27002:2013 and ABNT NBR ISO/IEC 27701:2020, recognized worldwide as a code of practice for information security management, as well as in accordance with the laws in force in our country, especially with Brazilian Law No. 13.709/2018, General Data Protection Law (LGPD).

2. OBJECTIVES

a. Establish guidelines that allow SciCrop's employees and customers to follow standards of behavior related to information security suited to the business needs and legal protection of the company and the individual.

b. To guide the definition of specific information security standards and procedures, as well as the implementation of controls and processes to meet them.

c. Preserve SciCrop's information regarding:

i. **Integrity:** guarantee that the information is kept in its original state, in order to protect it, in storage or transmission, against undue, intentional or accidental alterations.
ii. **Confidentiality:** guarantee that access to information is obtained only by authorized persons.
iii. **Availability:** ensuring that authorized users gain access to information and corresponding assets whenever necessary.

3. ISP-SciCrop APPLICATIONS

a. The guidelines established here must be followed by all employees, as well as service providers, and apply to information in any medium or support.

b. This policy informs each employee that the company's environments,

systems, computers and networks may be monitored and recorded, with prior information, as provided for in Brazilian law.

c. It is also the obligation of each employee to keep up to date with this policy and related procedures and standards, seeking guidance from his manager or IT area whenever he is not absolutely sure about the acquisition, use and/or disposal of information.

4. ISP-SciCrop PRINCIPLES

a. All information produced or received by employees as a result of the professional activity contracted by SciCrop belongs to that institution. Exceptions must be explicit and formalized in a contract between the parties.

b. Computer and communication equipment, systems and information are used by employees to carry out professional activities. Personal use of resources is permitted as long as it does not impair the performance of systems and services.

c. SciCrop, through the IT area, may record all use of systems and services, in order to guarantee the availability and security of the information used.

5. ISP-SciCrop REQUIREMENTS

a. For information uniformity, ISP-SciCrop must be communicated to all SciCrop employees so that the policy is complied with inside and outside the company.

b. There must be a committee responsible for the management of information security, hereinafter referred to as the Information Security Committee (CSI).

c. Both ISP-SciCrop and the standards must be periodically reviewed and updated, whenever any relevant fact or event motivates an extraordinary review, according to the analysis and decision of the Safety Committee.

d. All SciCrop contracts must include the annex to a Confidentiality Agreement or *Non-Disclosure Agreement* (NDA), or *Memorandum of Understanding* (MOU) that contains a Confidentiality Clause, as an essential condition for granting access information assets made available by the institution.

e. Responsibility for information security must be communicated at the stage of hiring employees. All employees must be instructed on safety procedures, as well as the correct use of assets, in order to reduce possible risks. They must sign a disclaimer.

f. Any incident that affects information security must be initially communicated to the IT area and, if deemed necessary, it must subsequently forward it to the Information Security Committee for analysis.

g. A contingency and continuity plan for the main systems and services must be implemented and tested, at least annually, in order to reduce the risk of loss of confidentiality, integrity and availability of information assets.

h. All information security requirements, including the need for contingency plans, must be identified in the scoping phase of a project or system, and justified, agreed upon, documented, implemented and tested during the execution phase.

i. Appropriate controls, audit trails or activity records must be created and instituted at all points and systems where the institution deems necessary to reduce the risks of its information assets, such as workstations, *notebooks*,

Internet access, electronic mail, commercial and financial systems developed by SciCrop or by third parties.

j. Production environments must be segregated and tightly controlled, ensuring the necessary isolation from development, testing and approval environments.

k. SciCrop disclaims any and all liability arising from the improper, negligent or reckless use of the resources and services provided to its employees, reserving the right to analyze data and evidence to obtain evidence to be used in the investigative processes, as well as adopt appropriate legal measures.

l. This policy will be implemented at SciCrop through specific procedures, mandatory for all employees, regardless of hierarchical level or function in the company, as well as employment relationship or service provision.

m. Failure to comply with the requirements set forth in this policy will result in a violation of the institution's internal rules and will subject the user to the appropriate administrative and legal measures.

6. SPECIFIC RESPONSIBILITIES

a. Of Collaborators in General

i. A collaborator is understood to be any and all natural person, contracted by CLT or service provider through a legal entity or not, who performs any activity inside or outside the institution.

ii. It will be the sole responsibility of each employee, any loss or damage that may suffer or cause to SciCrop and/or third parties, as a result of non-compliance with the guidelines and standards referred to herein.

b. Employees in Exception Regime (Temporary)

i. They must understand the risks associated with their special condition and strictly comply with what is foreseen in the acceptance granted by the Information Security Committee.

ii. The concession may be revoked at any time if it is verified that the business reason justification no longer compensates for the risk related to the exception regime or if the employee who received it is not complying with the conditions defined in the acceptance.

c. Personnel and/or Process Managers

i. Have an exemplary attitude in relation to information security, serving as a model of conduct for the employees under their management.

ii. Assign to employees, at the stage of hiring and formalizing individual employment, service or partnership contracts, the responsibility for complying with the ISP-SciCrop.

iii. Require employees to sign the Term of Commitment, assuming the duty to follow the established rules, as well as committing to maintain secrecy and confidentiality, even when disconnected, on all SciCrop information assets.

iv. Before granting access to the institution's information, require the signature of the Non-Disclosure Agreement from casual employees and service providers who are not covered by an existing contract, for example, during the survey phase for the presentation of commercial proposals.

v. Adapt the standards, processes, procedures and systems under their responsibility to comply with this policy.

d. Information Custodians

i. In the Systems and Applications Development Area

1. The systems and applications development area must ensure that every programmer, developer, systems analyst, computer scientist, data scientist, data engineer, requirements analyst and databases, and comply with this policy and implement secure systems development techniques.

2. The systems and applications development area must ensure that all systems development is done in segregated

environments, specific for programming, testing and finally production.

3. The systems and applications development area must ensure that there are safe methods of data transfer and storage in the systems development processes. With special attention to the use of PKI in data transfer using TLS version 1.2 or higher, through secure connections in its various development environments.

4. In addition to safe development environments, the systems and applications development area must ensure that employees involved in system development have training and practice in the use of safe development methods, in compliance with the OWASP Security Knowledge Framework.

5. The systems and applications development area must ensure that source code repositories have secure access methods segregated by user groups with MFA support.

6. Regarding the storage of passwords, systems that store user passwords can never be developed, whether in file systems or databases of any nature, the hashes of such passwords may be stored, provided that they are created by Argon2, Scrypt or Bcrypt algorithms using salt. As for security certificates used for signature, authentication or encryption, private keys of any kind should never be stored.

ii. From the Information Technology Area

1. Test the effectiveness of the controls used and inform managers of residual risks. Agree with managers the level of service that will be provided and incident response procedures.

2. Configure the equipment, tools and systems granted to employees with all the necessary controls to comply with the security requirements established by this policy.

3. Administrators and operators of computer systems can, due to their privileges as users, access the files and data of other users. However, this will only be allowed when it is necessary to carry out operational activities under your responsibility, such as maintaining computers, performing backups, audits or tests in the environment.

4. Segregate administrative and operational functions in order to restrict the powers of each individual to the minimum necessary, eliminating or at least reducing the existence of people who can exclude the logs and audit trails of their own actions.

5. Ensure special security for systems with public access, keeping evidence that allows traceability for audit or investigation purposes.

6. Generate and maintain audit trails with a level of detail sufficient to track potential failures and fraud. For trails generated and/or maintained in electronic media, implement integrity controls to make them legally valid as evidence.

7. Administer, protect and test backups of programs and data related to critical and relevant processes for SciCrop. Implement controls that generate auditable records for media removal and transport of information held by IT, in environments fully controlled by IT.

8. The information manager must be previously informed about the end of the retention period, so that he has the option of changing it before the information is definitively discarded by the custodian.

9. When internal movement of IT assets occurs, ensure that a user's information is not irretrievably removed before making the asset available to another user.

10. Plan, implement, supply and monitor the storage, processing and transmission capacity necessary to guarantee the security required by the business areas.

11. Assign each account or access device to computers, systems, databases and any other information asset to a responsible person identifiable as a natural person, whereby:

    a. individual users (*logins*) of employees will be the employee's own responsibility;
    b. users (*logins*) will be the responsibility of the contracting area manager.

12. Continuously protect all company information assets against malicious code, and ensure that all new assets enter the production environment only after they are free of malicious and/or unwanted code.

13. Ensuring that vulnerabilities or weaknesses are not introduced into the company's production environment in change processes, with code auditing and contractual protection being ideal for control and accountability in case of use by third parties.

14. Define formal rules for installing software and hardware in a corporate production environment, as well as in an exclusively educational environment, requiring compliance within the company.

15. Conduct periodic audits of technical configurations and risk analysis.

16. Be responsible for the use, handling, keeping of signatures and digital certificates.

17. Ensure, as quickly as possible, with a formal request, the blocking of user access due to company shutdown, incident, investigation or other situation that requires a restrictive

measure for the purpose of safeguarding the company's assets.

18. Ensure that all servers, stations and other devices with access to the company's network operate with the clock synchronized with the official time servers of the Brazilian government, regardless of zones and time zones.

19. Monitor the IT (Information Technology) environment, generating indicators and histories of:
    a. Use of the installed capacity of the network and equipment;
    b. Response time for accessing the internet and SciCrop's critical systems;
    c. Periods of unavailability in access to the internet and to SciCrop's critical systems;
    d. Security incidents (viruses, *trojans*, *spyware*, theft, unauthorized access, and so on);
    e. Activity of all employees while accessing external networks, including the internet (for example: websites visited, emails received/sent, upload/download of files, among others).

iii. From the Information Security Area

1. Propose specific methodologies and processes for information security, such as risk assessment and information classification system.

2. Propose and support initiatives aimed at securing SciCrop's information assets.

3. Publish and promote versions of ISP-SciCrop and Information Security Standards approved by the Information Security Committee.

4. Promoting employee awareness regarding the relevance of

information security to SciCrop's business, through campaigns, lectures, training and other *endomarketing*.

5. Support the assessment and adequacy of specific information security controls for new systems or services.

6. Critically analyze incidents together with the Information Security Committee.

7. Present the minutes and summaries of the Information Security Committee meetings, highlighting matters that require the intervention of the committee itself or other members of the board.

8. Maintain effective communication with the Information Security Committee on matters related to topics that affect or have the potential to affect SciCrop.

9. Seek alignment with the institution's corporate guidelines.

iv. The Information Security Committee (CSI)

1. It must be formally constituted by employees with a minimum managerial hierarchical level**,** appointed to participate in the group for a period of one year.

2. The minimum composition must include one employee from each of the relevant areas.

3. The committee shall formally meet at least once every six months. Additional meetings must be held whenever it is necessary to deliberate on a serious incident or definition relevant to SciCrop.

4. CSI may use specialists, internal or external, to support matters that require specific technical knowledge.

5. CSI is responsible for:

a. Proposing investments related to information security in order to further reduce risks;
b. Propose changes to ISP-SciCrop versions and the inclusion, elimination or change of complementary rules;
c. Evaluate security incidents and propose corrective actions;
d. Define the appropriate measures in cases of non-compliance with the ISP-SciCrop and/or the complementary Information Security Standards.

e. Environmental Monitoring and Auditing

i. To ensure the rules mentioned in this ISP-SciCrop, SciCrop may:

1. Implement monitoring systems in workstations, servers, electronic mail, internet connections, mobile or wireless devices and other network components – the information generated by these systems may be used to identify users and their respective accesses, as well as manipulated material;

2. Make public the information obtained by the monitoring and auditing systems, in the event of a legal requirement, at the request of the manager (or superior) or by determination of the Information Security Committee;

3. Carry out, at any time, physical inspection on the machines owned by it;

4. Install protective, preventive and detectable systems to ensure the security of information and access perimeters.

7. ELECTRONIC MAIL

a. The purpose of this rule is to inform SciCrop's employees what are the permitted and prohibited activities regarding the use of corporate electronic mail.

b. The use of SciCrop's e-mail is for corporate purposes and related to the user's activities within the institution. The use of this service for personal purposes is allowed as long as it is done with common sense, does not harm the company and also does not generate an impact on network traffic.

c. We add that employees are prohibited from using SciCrop's electronic mail to:

i. Send unsolicited messages to multiple recipients, unless related to the institution's legitimate use;
ii. Send an e-mail message from your department's address or using another person's username or e-mail address that you are not authorized to use;
iii. Send any message by electronic means that makes its sender and/or SciCrop or its units vulnerable to civil or criminal action;
iv. Disclose unauthorized information or screenshots, systems, documents and the like without express and formal authorization granted by the owner of that information asset;
v. Falsify address information, tamper with headers to hide the identity of senders and/or recipients, in order to avoid the prescribed punishments;
vi. Delete pertinent e-mail messages when any of SciCrop's units are subject to some type of investigation;
vii. Produce, transmit or disseminate a message that:

viii. Contains any act or provides guidance that conflicts with or is contrary to SciCrop's interests;
ix. Contain electronic threats such as: spam, *mail bombing*, computer viruses and the like;
x. Contain files with executable code: (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) or any other extension that represents a security risk;
xi. Intends to gain unauthorized access to another computer, server or network;
xii. Aims to disrupt a service, servers or computer network through any illicit or unauthorized method;
xiii. Aim to circumvent any security system, internal or external to the

company;

xiv. Aims to secretly surveil or harass another user;
xv. Aim to access confidential information without the owner's explicit authorization;
xvi. Aims to improperly access information that may cause harm to anyone;
xvii. Include encrypted, encoded, masked images or using a technological means/resource intended to hide content;
xviii. Contain attachment(s) of a size greater than the limit offered by the electronic mail system, whether for sending or receiving, as well as using the mail system as a means of storing files;
xix. Has content deemed inappropriate, obscene or illegal;
xx. Be libelous, defamatory, degrading, infamous, offensive, violent, threatening, pornographic, among others;
xxi. Contain prejudiced persecution based on sex, race, physical or mental disability or other protected status;
xxii. Has local or country political ends (political propaganda);
xxiii. Include copyrighted material without permission from the rights holder.

d. E-mail messages must always include a standardized signature, in the following format:

i. Name of employee
ii. Position
iii. Contact numbers (landline and mobile)
iv. Company web
v. address Company physical address

8. INTERNET

a. All current SciCrop rules are basically aimed at developing a behavior eminently ethical and professional use of the Internet. Although the direct and permanent connection of the institution's corporate network to the Internet offers great potential for benefits, it opens the door to significant risks for information assets. Any information that is accessed, transmitted, received or produced on the internet is subject to disclosure and auditing. Therefore, SciCrop, in full legal compliance, reserves the right to monitor and

record all access to it.

b. The equipment, technology and services provided for internet access are the property of the institution, which can analyze and, if necessary, block any file, website, email, domain or application stored on the network/internet, whether on a local disk, at the station or in private areas of the network, in order to ensure compliance with its Information Security Policy.

c. SciCrop, by monitoring the internal network, intends to ensure the integrity of data and programs. Any attempt to change the security parameters, by any employee, without proper accreditation and authorization to do so, will be deemed inappropriate and the related risks will be informed to the employee and the respective manager. The use of any resource for illegal activities may lead to administrative actions and penalties arising from civil and criminal proceedings, in which case the institution will actively cooperate with the competent authorities.

d. The internet provided by the institution to its employees, regardless of their contractual relationship, can be used for personal purposes, as long as it does not interfere with the progress of work at the units.

e. As it is in SciCrop's interest that its employees are well informed, the use of news sites or services, for example, is acceptable, as long as it does not compromise network bandwidth during strictly business hours, does not disturb the smooth running of the work or imply conflicts of interest with your business objectives.

f. Only employees who are duly authorized to speak on behalf of SciCrop to the media may express themselves, whether by *email*interview *online*, *podcast*, physical document, among others.

g. Only employees authorized by the institution may copy, capture, print or send screen images to third parties, and must comply with the internal rules for the use of images, the Copyright Law, the protection of the image guaranteed by the Federal Constitution and other legal provisions.

h. Undue disclosure and/or sharing of information in the administrative area on discussion lists, *websites* or relationship communities, chat rooms ,instant

communicators or any other related technology that may appear on the internet is prohibited.

i. Employees with internet access will only be able to *download* (download) programs directly linked to their activities at SciCrop and must provide whatever is necessary to regularize the license and registration of these programs, provided they are authorized by their direct manager.

j. Unauthorized use, installation, copying, or distribution of *software* that is copyrighted, trademarked, or patented on the Internet is expressly prohibited. Any *software* unauthorized

k. Employees may not, under any circumstances, use SciCrop's resources to *download* or distribute *software* or data, an activity considered criminal according to national legislation.

l. The *download* and use of entertainment programs, music or similar (in any format) may be performed by users who have professional activities related to these categories. To this end, security groups, whose members must be defined by the respective managers, need to be created in order to enable this special access. Upon request and approval of the responsible technical area, the use of these resources will be released under an exception regime, when they are intrinsic to the company's activities, as well as occasional practices, such as events, symposia and/or any other actions carried out that are entitled to this need.

m. As a general rule, sexual material may not be displayed, stored, distributed, edited, printed or recorded through any resource. If necessary, security groups must be created to enable this special user profile and its members defined by the respective managers.

n. Collaborators with internet access may not *upload* (upload) any software licensed to SciCrop or data owned by them to their partners and customers, without express authorization from the person responsible for the *software* or data.

o. Employees may not use SciCrop's resources to deliberately propagate any type of virus, *worm*, trojan horse, *spam*, harass, disrupt or control other

computer programs.

p. access to *software peer-to-peer* (*BitTorrent* and the like) will not be allowed.services *Streaming* radios *online*channels *broadcast* and the like) will be allowed to specific groups. Instant communication services are available for internal use and through a tool approved by the company. Such communication is monitored and may be used at any time for legal purposes and linked to the rules described in this document. The use of unauthorized means of instant communication through unauthorized mobile devices linked to the corporate network is prohibited and is subject to the application of current laws. The dissemination of corporate, confidential content, as well as actions of a pejorative nature, published in instant communicators and/or social media or other unnamed, private or public media, will be the object of actions under the law.

q. Access to *proxy*, *bypass*, anonymization networks and/or identity concealment features, as well as virtual private networks, is not allowed, except in situations previously discussed with the Information Security Committee.

r. Access to *applets* and *web* or solutions installed in connection with the equipment, operating system, *software* in general or *software* , which offer remote access to devices present on the internal or external network, Internet or clients is prohibited.

s. Under specific customer requests to meet data integrations, exceptions may be made to meet the need for interconnection with third-party systems such as Microsoft Power BI, Tableau and Qlik, where public access networks, reading credentials, and eventual permissions in white lists.

9. IDENTIFICATION

a. Identification devices and passwords protect the identity of the user employee, preventing and preventing a person from impersonating another before SciCrop and/or third parties.

b. The use of another person's identification devices and/or passwords constitutes a crime typified in the Brazilian Penal Code (art. 307 - false

identity).

c. This rule aims to establish responsibility criteria for the use of identification devices and should be applied to all employees.

d. Todos os dispositivos de identificação utilizados na SciCrop, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

e. The user, linked to such identifying devices, will be responsible for their correct use before the institution and the legislation (civil and criminal).
Any and all personal identification devices, therefore, cannot be shared with other people under any circumstances.

f. If there is a login for use shared by more than one employee, the responsibility before SciCrop and the legislation (civil and criminal) will be of the users who use it. Only if knowledge or a request from the shared use manager is identified, he should be held accountable.

g. Login sharing for system administration functions is prohibited.

h. SciCrop's Human Resources (HR) Department is responsible for issuing and controlling employees' physical identity documents.

i. The IT Management is responsible for creating the logical identity of the employees in the institution, under the terms of the Procedure for Managing Group and User Accounts.

j. Visitors, interns, temporary employees, regular employees and service providers, whether individuals and/or legal entities, must be distinctly identified. When performing the first access to the local network environment, the user must immediately change his password according to the guidelines presented.

k. Users who do not have an administrator profile must have a variable-length password, with at least 8 (eight) alphanumeric characters, using special

characters (@ # $ %) and variation between uppercase and lowercase (upper and lowercase) always that possible.

l. Users who have an administrator profile or privileged access must use a password of at least 10 (ten) characters, alphanumeric, using special characters (@ # $ %) and variation of uppercase and lowercase (upper and lowercase) necessarily.

m. Each user is responsible for memorizing their own password, as well as protecting and guarding the identification devices assigned to them.

n. Passwords must not be written down or stored in electronic files (Word, Excel, etc.), understandable by human language (not encrypted); should not be based on personal information, such as own name, family name, date of birth, address, license plate, company name, department name; and should not consist of obvious keyboard combinations, such as “abcdefgh”, “87654321”, among others.

o. After 3 (three) access attempts, the user's account will be locked. For unlocking it is necessary for the user to contact SciCrop's IT Management. A process for password renewal (confirming identity) must be established.

p. Users can change their own password, and should be instructed to do so, if they suspect that third parties have gained unauthorized access to their login/password.

q. The maximum frequency for changing passwords is 45 (forty-five) days, and the last 3 (three) passwords cannot be repeated. Critical and sensitive systems for the institution and logins with administrative privileges must require password changes every 30 days. Systems must force passwords to be changed within this maximum timeframe.

r. All accesses must be blocked immediately when they become unnecessary.

s. Therefore, as soon as any user is fired or requests resignation, the Human Resources Department must immediately communicate this fact to the Information Technology Department, so that this action can be taken. The same conduct applies to users whose contract or provision of services has

ended, as well as test users and other similar situations.

t. If the employee forgets his password, he must formally request the change or appear in person at the responsible technical area to register a new one.

10. COMPUTERS AND TECHNOLOGICAL RESOURCES

a. The equipment available to employees is the property of SciCrop, and it is up to each one to use and handle them correctly for activities of interest to the institution, as well as comply with the recommendations contained in the operational procedures provided by the responsible management.

b. Any physical or logical maintenance procedure, installation, uninstallation, configuration or modification, without the prior knowledge and follow-up of a technician from SciCrop's IT Management, or whomever he determines, is prohibited. The managements that need to carry out tests must previously request them to the IT Management, being legally and technically responsible for the actions carried out.

c. All operating system or application security updates and corrections can only be made after due validation in the respective approval environment, and after their availability by the manufacturer or supplier.

d. Systems and computers must have versions of antivirus software installed, activated, and permanently updated. The user, in case of suspicion of a virus or problems in functionality, must contact the responsible technical department by registering a call at the service desk.

e. The transfer and/or disclosure of any software, program or computer instructions to third parties, by any means of transport (physical or logical), can only be carried out with the proper identification of the applicant, if positively verified and in accordance with the classification of such information and the real need of the recipient.

f. Personal files and/or files not relevant to SciCrop's business (photos, music, videos, etc.) should not be copied/moved to network drives, as they may overload the storage on the servers. If the existence of these files is identified, they may be permanently deleted by means of prior

communication to the user.

g. Essential documents for the activities of the institution's employees must be saved on network drives. Such files, if recorded only locally on computers (for example, on the C: drive), are not guaranteed to be backed up and may be lost in the event of a computer failure, thus being the user's own responsibility.

h. SciCrop employees and/or holders of privileged accounts must not execute any type of command or program that may overload existing services on the corporate network without the prior request and authorization of the IT Management.

i. When using computers, equipment and IT resources, some rules must be met:

j. All computers for individual use must have a Bios/Setup password to restrict access by unauthorized employees. Such passwords will be defined by SciCrop's IT Management, which will have access to them for equipment maintenance;

k. Employees must inform the technical department of any identification of a strange device connected to their computer;

l. It is forbidden to open or handle computers or other computer equipment for any type of repair that is not carried out by a technician from SciCrop's IT Management or by third parties duly hired for the service;

m. All internal or external modems must be removed or disabled to prevent intrusion/evasion of information, programs, viruses. In some special cases, according to a specific rule, the possibility of use for contingency plans will be considered with the authorization of the managers of the areas and the IT area;

n. It is expressly forbidden to consume food, drink or smoke at the work table and close to equipment;

o. The employee must maintain the configuration of the equipment provided by

SciCrop, following the appropriate security controls required by the Information Security Policy and by the specific rules of the institution, assuming responsibility as custodian of information;

p. All computer terminals and printers must be password-protected (locked), under the terms provided for by the Authentication Standard, when they are not being used;

q. All technological resources acquired by SciCrop must immediately have their default passwords changed;

r. The equipment must keep the records of events safely preserved, including the identification of employees, dates and times of access.

s. We have added some situations in which the use of SciCrop computers and technological resources is prohibited:
   i. Attempt or gain unauthorized access to another computer, server or network;
   ii. Bypass any security systems;
   iii. Access confidential information without the owner's explicit authorization;
   iv. Secretly surveillance others by electronic devices or software, such as packet analyzers (sniffers);
   v. Disrupt a service, servers or computer network through any illicit or unauthorized method;
   vi. Use any type of technological resource to commit or be an accomplice in acts of violation, sexual harassment, disturbance, manipulation or suppression of copyright or intellectual property without the due legal authorization of the owner;
   vii. Host pornography, racist material or any other material that violates the legislation in force in the country, morals, good customs and public order;

viii. Using pirated software, an activity considered criminal according to national legislation;

ix. Use email servers not managed by SciCrop, insecure FTP or removable media such as Pen Drives, CDs and DVDs as a way of transmitting data.

11. MOBILE DEVICES

a. SciCrop wants to facilitate mobility and the flow of information among its employees. So it allows them to use portable equipment.

b. When “mobile device” is described, it means any electronic equipment with mobility assignments owned by the institution, or approved and allowed by its IT Management, such as: notebooks, smartphones, tablets, flash drives and the like.

c. This standard aims to establish criteria for handling, prevention and responsibility for the use of mobile devices and should be applied to all employees who use such equipment.

d. SciCrop, as the owner of the supplied equipment, reserves the right to inspect it at any time, if safety maintenance is required.

e. The employee, therefore, undertakes not to use, reveal or disclose to third parties, in any way, directly or indirectly, for their own benefit or that of third parties, any information, confidential or not, that they have or will have knowledge due to their functions at SciCrop, even after the contractual relationship with the institution has ended.

f. Every employee must periodically perform a backup of the data on their mobile device. You should also keep these backups separate from your mobile device, i.e. do not upload them together.

g. Technical support for mobile devices owned by SciCrop and its users must follow the same support flow contracted by the institution.

h. Every employee must use automatic lock passwords for their mobile device. It will not be allowed, under any circumstances, to change the configuration of

the equipment's operating systems, especially those referring to security and the generation of logs, without proper communication and authorization from the responsible area and without the conduction, assistance or presence of a IT Management technician.

i. The employee must be responsible for not maintaining or using any programs and/or applications that have not been installed or authorized by a technician from SciCrop's IT Management.

j. Unauthorized reproduction of software installed on mobile devices provided by the institution will constitute misuse of the equipment and legal infringement of the manufacturer's copyright.

k. The use of broadband networks is allowed in locations known to the employee, such as: his/her home, hotels, suppliers and customers, provided that the employee maintains common data security practices, not revealing sensitive data, passwords, codes and keeping an eye on the characteristics of websites accessed, in order to prevent data theft tactics such as phishing and the like. In case of using a public network, it is recommended to use a virtual private network service that may, if necessary, be provided by the company.

l. It is the employee's responsibility, in the event of theft or theft of a mobile device provided by SciCrop, to immediately notify their direct manager and IT Management.

m. You should also seek the help of law enforcement authorities by filing a police report as soon as possible.

n. The employee must be aware that the misuse of the mobile device will characterize the assumption of all risks of its misuse, being solely responsible for any damages, direct or indirect, present or future, that may cause SciCrop and/or the third parties.

o. Employees who wish to use private portable equipment or purchase accessories and subsequently connect them to the SciCrop network must previously submit such equipment to the IT Management authorization process.

p. Portable equipment, such as smartphones, tablets, flash drives and players of any kind, when not provided to the employee by the institution, will not be validated for use and connection in its corporate network.

12. DATACENTER (LOCAL PHYSICAL, REMOTE PHYSICAL, REMOTE VIRTUAL IN CLOUD)

a. Access to the Datacenter or place reserved for information technology and telecommunications equipment must only be done through a strong authentication system. For example: biometrics, magnetic card among others.

b. All access to the Datacenter, through the strong authentication system, must be registered (user, date and time) using its own software.

c. An audit of access to the Datacenter must be performed weekly through the log system report.

d. The “administrator” user of the strong authentication system will be owned and managed by the infrastructure coordinator, in accordance with the Administrative Accounts Control Procedure.

e. The list of roles entitled to access the Datacenter must be constantly updated, in accordance with the Datacenter Access Control Procedure, and saved in the network directory.

f. In locations where there are no employees in the information technology area, people from other departments must be registered in the access system so that they can carry out operational activities within the Datacenter, such as: exchange of backup tapes, support in eventual problems, and so on.

g. Access by visitors or third parties can only be carried out with the accompaniment of an authorized employee, who must complete the access request provided for in the Datacenter Access Control Procedure, as well as sign the Term of Responsibility.

h. Access to the Datacenter, by means of a key, can only occur in emergency situations, when the physical security of the Datacenter is compromised, such as by fire, flood, damage to the building structure or when the strong

authentication system is not working.

i. If there is a need for non-emergency access, the requesting area must request authorization in advance from any employee responsible for managing access release, according to the list saved in the Datacenter Access Control Procedure.

j. There must be two copies of Datacenter door keys. One of the copies will be in the possession of the coordinator responsible for the Datacenter, the other, in the possession of the infrastructure coordinator.

k. The Datacenter must be kept clean and organized. Any procedure that generates garbage or dirt in this environment can only be carried out with the collaboration of the General Services Department.

l. The entry of any type of food, drink, smoke or flammable product is not allowed.

m. The entry or removal of any equipment from the Datacenter will only occur with the completion of the release request by the requesting employee and the formal authorization of this instrument by the person responsible for the Datacenter, in accordance with the terms of the Equipment Control and Transfer Procedure.

n. In the event of termination of employees or collaborators who have access to the Datacenter, their exclusion from the strong authentication system and from the list of authorized employees must immediately be provided, in accordance with the process defined in the Datacenter Access Control Procedure.

13. BACKUP

a. All backups must be automated by automated scheduling systems so that they are preferably performed outside business hours, in so-called “backup windows” – periods in which there is little or no access by users or automated processes to computer systems.

b. Employees responsible for managing backup systems must carry out frequent research to identify patch updates, new product versions, life cycle (when the

software will no longer have the manufacturer's warranty), suggestions for improvements, among others.

c. Backup media (such as DAT, DLT, LTO, DVD, CD and others) must be stored in a dry, climate-controlled, safe place (preferably in fire-safes according to ABNT standards) and as far away from the Datacenter as possible.

d. Backup media must be properly identified, including when it is necessary to make name changes, and preferably with non-handwritten labels, giving a more organized and professional connotation.

e. The lifetime and use of backup media must be monitored and controlled by those responsible, with the objective of excluding media that may present recording or restoration risks resulting from prolonged use, beyond the period recommended by the manufacturer.

f. It is necessary to forecast, in an annual budget, the renewal of the media due to its natural wear and tear, as well as a constant stock of media for any emergency use.

g. Media that has errors must first be formatted and tested. If the error persists, they should be discarded.

h. It is necessary to periodically insert the wiper device into the backup drives in accordance with the Backup Media Control Procedure.

i. Historical or special backup media must be stored in secure facilities, preferably with a safe-room structure, at least 10 kilometers away from the Datacenter.

j. Essential, critical backups for the proper functioning of SciCrop's business require a special retention rule, as provided for in the specific procedures and in accordance with the Information Classification Standard, thus following the tax and legal provisions existing in the country.

k. In the event of a backup and/or restore error, it must be done at the first available time, as soon as the person in charge has identified and resolved the problem.

l. If the impact of the slowness of the systems derived from this backup is extremely negative, they must be authorized only when justified under the terms of the Backup and Restore Control Procedure.

m. Any delays in performing a backup or restore must be formally justified by those responsible under the Backup Media Control Procedure.

n. Backup restore tests must be performed by those responsible, in accordance with the specific procedures, approximately every 30 or 60 days, according to the criticality of the backup.

o. As it is a simulation, the executor must restore the files in a different location from the original, so that the valid files do not overlap.

p. In order to formalize the control of the execution of backups and restores, there must be a rigid control form for the execution of these routines, which must be completed by those responsible and audited by the infrastructure coordinator, pursuant to the Backup and Restore Control Procedure.

q. The responsible employees described in the appropriate procedures and in the responsibility worksheet may delegate the operational task to a custodian when, for reasons of force majeure, they cannot operate. However, the custodian cannot exempt itself from the responsibility of the process.

14. FINAL PROVISIONS

a. Like ethics, safety must be understood as a fundamental part of SciCrop's internal culture. That is, any security incident is implied as someone acting against ethics and good customs governed by the institution.