SECURITY POLICY AND CONTROL INFORMATION - PSCI

The Security and Information Control Policy also referred to as PSCI is the document that guides and sets standards and conducts, in Bitcoin To You, for the control and protection of information and legal responsibility for all users that, if doing this so organic in the organization's culture.

I - REFERENCE PSCI

This PSCI is based on recommendations and listed control objectives by the ABNT NBR ISO / IEC 27002/2005, recognized worldwide as a code of practice for information security management, and is in accordance with the NIST Framework and its publications Information Security and legal regulations in force in the country.

II - RELEVANCE OF PSCI

the Bitcoin To You information systems as well as your data network suffer various types of threats to information security, as cyber criminals, malware, hackers and various types of denial of service attacks are becoming more frequent and incredibly sophisticated. This reality that extends not only to Bitcoin To You, but for exchanges in general, is critical, and because of this the relevance of having a PSCI well grounded and rooted in the organizational culture.

It is understood that not only have a PSCI, have it well grounded in the company's culture, it should be applied daily and controlled because the risks to security are changing and with them the Bitcoin To You is modified as well, giving more relevance and importance of the safety of its operations.

III - OBJECTIVES

The purpose of the PSCI is to establish guidelines that allow customers, suppliers and employees of Bitcoin To You follow behavior patterns that ensure the maintenance of security and control as the information commonly used and processed in the business.

To achieve this goal it is necessary that such behaviors violate the specific rules and procedures for information security and consistent with the controls for the maintenance and management of information. In this sense the general aim is dismembered the following specific objectives.

- Integrity: the information must preserve its original state, and be fully protected as the improper, intentional or accidental changes. Controls and processes should ensure the integrity of their own design of products and systems Bitcoin To You.
- Confidentiality: not allowed any hiring employees without signing Secrecy and Confidentiality Agreement, in addition, it is prohibited any provision of customer information, contracts, and other processes to third parties unless required by law. The other customer information is accessed only by themselves.
- Availability: users are ensured access information that is relevant to themselves, while also ensuring the confidentiality and integrity of our content.

IV - APPLICATION OF PSCI

The guidelines set forth herein should be followed by all employees (regardless of busy hierarchical level), customers and service providers of Bitcoin To You, and apply to information in any medium or support.

It is the duty of each employee to keep updated as standards, application and updating of the PSCI and the related procedures, seeking guidance manutentor the PSCI where there is doubt, or in case you're in doubt, the front being the situation of acquisition , use and / or disposal information.

V - Principles of PSCI

The guiding principles of PSCI are:

- Principle of Production and Property Information: Bitcoin To You carries on business with large volume of production information. This principle takes into account that all information produced as a result of the professional activity of the company belong to the same, with some exceptions, formalized between the related parties.
- Principle of Resource Utilization: All equipment that travel information such as computer equipment, communication systems, sofwares among others, may be used by employees as long as they use with integrity, confidential and secure, in accordance with the objectives set in PSCI.
- Principle of Information Security: The Bitcoin To You in the exercise of PSCI may register accesses, disposals, additions, acquisitions, changes and use of information in order to ensure the availability and security of information in accordance with the objectives set in the PSCI.

VI - REQUIREMENTS PSCI

The requirements for Security Policy and Information Control those listed below:

- Said policy should be communicated and made available to all employees of Bitcoin To You so that it be complied with within and outside the organization;
- It shall constitute a multidisciplinary committee responsible for the management and control of information security, called COMMITTEE INFORMATION SECURITY;
- The PSCI should be updated and reviewed periodically or whenever a supervening fact occurs, motivating early review;
- All contracts practiced by Bitcoin To You must be preceded clause Confidentiality and Confidentiality Agreement;
- All employees at the time of admission shall be notified about the PSCI and should also sign the Secrecy and Confidentiality Agreement. In

addition to the signature they should be instructed on safety procedures and the correct handling of information equipment, systems, software, media and others, in order to minimize the potential protection of information;

- In case of incidents affecting information security, these should be reported to manutentor the PSCI and forwarded to the Information Security Committee for review;
- They should be established tools of control and information security management;
- It should be implemented action plan for monitoring of computer equipment, media, and other systems in order to advance to act in situations of possible risks to information;
- Failure to comply with the requirements of PSCI entail violation of internal rules of Bitcoin to You and may cause administrative measures and appropriate legal.

VII - ORGANIZATION AND THE PSCI specific responsibilities

- directors

Have exemplary attitude in relation to information security, actively supporting the information security culture as strategic value of Bitcoin To You.

Set Security strategies Information, aligning the same to other business strategies.

Require employees to sign the Confidentiality Agreement and Confidentiality and compliance with the guidelines and standards set by the PSCI.

Decide on the creation and regulation of the Information Security Committee.

Regular intervals and / or whenever necessary meetings with the Information Security Committee.

Sign and approve documents that comply with the guidelines of the PSCI.

- Contributors

It is understood by all employees and any individual, contracted via CLT or service provider through corporate or not exercising any activity inside or outside the Bitcoin To You.

Employees should be responsible and should be organized to meet and comply strictly with the said PSCI.

Should be aware that any harm or damage that may suffer or cause Bitcoin To You and / or third parties as a result of non-compliance to the guidelines and standards set by the PSCI.

They must be alert and report to come across practices in non-compliance with PSCI, helping even the reeducation of habits in non-compliance.

Report to the Security Committee of Information suspicion or hint of violation of the rules and guidelines laid down in that instrument, failures in information security controls, breaking attempts at secrecy or confidentiality of information, or any other activity that goes contrary to the application the preferred PSCI.

- Information Security Committee

The Information Security Committee should be formally constituted by a minimum hierarchical management level professionals appointed to join the group for a period of one year.

Should create policies and procedures to ensure the control and security of information in Bitcoin To You. Should analyze the situations of non-conformities and risks to information security.

Should monitor the implementation of preventive monitoring of the action plan of information security and meet formally at least once every six months. Additional meetings shall be held whenever necessary.

Review the PSCI whenever necessary and provide training and updating of employees and stakeholders. If necessary you can use experts, internal or external, to support in matters requiring specific technical knowledge.

Must provide training to employees and parties involved in periods of 24 to 24 months to ensure recycling of the same aiming Mays efficient control and information security.

Review and control procedures for disaster recovery, disaster and response to incidents affecting the availability of information systems of Bitcoin To You.

Articulate and promote the culture of control, protection and information security within the Bitcoin To You and the entire chain of business relationships.

Manage conducting periodic vulnerability testing, including the internet and intranet of the company in order to identify existing threats and apply the necessary corrections for any vulnerability exposed.

VIII - MANAGEMENT AND CONTROL INFORMATION

- Area Information Technology

Test the effectiveness of controls used and inform the residual risk managers.

Waking up to managers the level of service to be provided and the response procedures to incidents.

Set up the equipment, tools and systems granted to employees with all the controls necessary to meet safety requirements established by this PSCI.

Administrators and operators of computer systems can, for the characteristic of their privileges as users access the files and data from other users. However, this will only be allowed when necessary for the implementation of operational activities under their responsibility, for example, maintenance of computers, performing backups, audits or testing in the environment.

Segregate the administrative and operational functions to restrict to a minimum the powers of each individual and eliminate or at least reduce, the existence of people who can delete the logs and audit trails of their own actions.

Ensure special security systems for public access as the management software, purchase and sale of criptoativos, making evidence guard to allow traceability for audit purposes or research.

Generate and maintain audit trails with sufficient level of detail to track possible failures and fraud. For the generated paths and / or maintained electronically, deploy integrity controls to make them legally valid as evidence.

Manage, protect and test the backup of programs and data related to critical processes and relevant to Bitcoin To You. Implement controls that generate auditable records for removal and transportation of media from custody information for IT in totally controlled environment for her.

Assign each account or device access to computers, systems, databases and any other asset information to a responsible identifiable as individuals, as follows:

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

Continually protect all enterprise information assets against malicious code, and ensure that all new assets only come to the production environment after they are free of malicious code and / or unwanted.

Ensure they are not released vulnerabilities or weaknesses in the company's production environment change processes, ideal code audit and contractual protection for control and accountability in the case of use of third parties.

Set formal rules for installing software and hardware in corporate production environment, requiring compliance within the company.

Conduct periodic audits of technical configurations and risk analysis.

Take responsibility for the use, handling, signing guard and digital certificates.

Ensure, as quickly as possible, with formal request user access blocking by the company shutdown reason, incident, investigation or other situation requiring restrictive measure for the purpose of safeguarding the company's assets.

Ensure that all servers, workstations and other devices with access to the company network operate with the clock synchronized with the official time servers of the Brazilian government.

Monitor the IT environment, generating historical and indicators:

a) use of the installed capacity of the network and equipment;
b) response time access to internet and critical systems of Bitcoin To You;
c) downtime in Internet access and critical systems of Bitcoin To You;
d) security incidents (viruses, Trojans, theft, unauthorized access, and so on);
e) activity of all employees during the access to external networks, including the Internet (eg, websites visited, e-mails received / sent, upload / download files, etc.).

- Security Area Information

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

Propose and support initiatives aimed at the security of the assets of Bitcoin To You information. Publish and promote versions of PSCI and Information Security Standards approved by the Information Security Committee.

Promote awareness of employees regarding the importance of information security to the business of Bitcoin To You, through campaigns, lectures, training and other internal marketing means.

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

Critically analyze incidents in conjunction with the Information Security Committee.

To present the minutes and summaries of meetings of the Information Security Committee, highlighting the issues that require intervention of the committee itself or other board members.

Maintain effective communication with the Information Security Committee on matters related to the subject that affect or have the potential to affect the Bitcoin To You.

Search alignment with corporate guidelines of the institution.

XIX - MONITORING AND AUDIT OF THE ENVIRONMENT

To ensure the rules mentioned in this PSCI the Bitcoin To You can:

- implement monitoring systems to workstations, servers, electronic mail, internet connections, mobile or wireless devices and other network

components - the information generated by these systems can be used to identify users and their made access as well as handled materials ;

- make public the information obtained by monitoring and auditing systems, in the case of judicial requirement, manager's request (or higher) or prescribed by the Information Security Committee;
- make, at any time, physical inspection on the machines of their property;
- install protection systems, preventive and detectable to ensure information security and access perimeters.

STORAGE AND TRANSMISSION OF CONFIDENTIAL INFORMATION

Given the contractual requirements of confidentiality, previously approved storage media are encrypted disks, transmission network or the Internet using SSL (with certificate of origin and destination of belonging transmitting to the parties agreed in the contract), SSH or SFTP (FTP over SSH) . For transmission of confidential information via email on different servers and domains, you need to add additional encryption at the file level (the password file using strong encryption AES least 1024 bits or equivalent). Password protection should be applied INCLUSIVE for protection of private certificates of general use (for example, to generate pairs of SSH keys, you must apply STRONG password in the private keys).

They should be classified as confidential information which in origin, nature or importance should not be shared or made available to unauthorized persons. Deemed to be confidential information so that all are classified as well - without distinction - data received or compiled from / to customers, passwords, financial or salary information, source code, sensitive information of users among others.

SECRET: information classified as SECRET have the highest level of sensitivity and criticality to the business. bitcoin wallets in general, encryption keys (SSL or SSH keys certificates) and general access credentials are examples of SECRET information. Other strategic information with a high level of confidentiality can also be classified as SECRET the discretion of the owner of the information.

Information on your possible leak implies direct financial impact to the business or jeopardize business continuity is an indication that she receives the maximum protection classification: SECRET.

The secret information usually have the following controls and protections:

a) They are stored in cryptographic volumes plus file encryption: multilevel encryption with keys and different algorithms.
b) Access to SECRET information is made whenever possible in OFFLINE equipment in a controlled environment with no other actors are not in the room.
c) The SECRET information may not be copied, photographed, filmed (including CCTV systems) or witnessed in person or via telepresence anyway.
d) Some secret information can not simply be stored (brain only storage), processed or transmitted in Bitcoin To You computational environment where this is possible.
e) Portfolio transactions flow criptomoedas (hot wallets): can only be stored in production using strong encryption in addition to the disk encryption servers and should only be read in its open format on the same server memory and temporarily to the time strictly necessary transactions drives Bitcoin to You and your customers.
f) criptomoedas portfolios reservation or custody (cold wallets): Storage is offline, access is via offline device.

The classification of documents should occur in the visible field, preferably on the first page and the next document header.

When a document contains more than one type of information with different original classification, for example, two documents together in a single file, the most restrictive classification takes effect for the entire document.

Any information that does not have its classification especificadade clearly in the document will be automatically considered as information "RESTRICTED".

RATING ASSIGNED TO INFORMATION INITIAL

It will be up to the developer AUTHOR information defining the access, permission levels and forms of protection when it is a RESTRICTED information, CONFIDENTIAL or SECRET.

Will be considered as information AUTHOR the employee who first produce or manipulate information within the Bitcoin To You environment.

Every employee will be responsible for classification and storage, following the recommendations contained herein.

It will be up to information security, providing technical support to the authors of the information generated and perform the appropriate training on data protection and storage insurance.

The area of Information Technology is a provider of resources and means to secure such information storage, as well as access control tools, protection and encryption.

OPEN FOR PUBLICATION INFORMATION

Only the managers of Bitcoin To You, with due assistance in the areas of communication and marketing, may classify information to disclose or externally set to Public Information.

USE OF TOOLS CORPORATE

The Bitcoin To You may provide the employee e-mail accounts, Internet access and other communication and productivity tools for streamlining work or utensils

such as drawers, cupboards and any physical or logical device for the implementation of work.

The use of these tools will be subject to this information security policy and access restrictions, according to the level of access granted to the user and decisions of the Information Security Committee.
As level of access to information policy, we use the premise of "least privilege possible." The developer will only have access to the applications and information that is strictly necessary for carrying out their work.

It is forbidden the use of any corporate resource, computers, networks, access and any corporate media to the commission of any unlawful act under penalty of civil liability or even criminal.

ACCESS AND INTERNET USE

The Bitcoin To You may allow browsing of content and access to Internet sites, always in accordance with your information security policy and blocks sites classified as unsafe or unreliable.

It is explicitly forbidden to transfer files through any protocol, application or tool that have not been previously and explicitly approved by the area if security of the Bitcoin To You info.

This approval is actually a tool of security analysis and product provider, in order to guarantee that only tools and manufacturers who have high maturity in information security, data protection and clear privacy policies to be incorporated into the list of tools and approved suppliers.

This prevents the inheritance of vulnerabilities through unsafe and untested tools, as well as partnerships with suppliers who can not follow the good information security practices.

Similarly, it will not be allowed to download copyrighted materials or installing unapproved software by Security Area Information.

E-MAIL / E-MAIL

The electronic mail of Bitcoin To You, like all communication platforms used in the company are working tools and should not be used for other purposes.

The information contained in electronic messages are owned by Bitcoin To You may be monitored at any time without warning or notice for compliance audit purposes to the internal rules, regulations and best practices applied to the Bitcoin To You business.

It is expressly forbidden to send classified information as "INTERNAL" and "CONFIDENTIAL" to email addresses outside of the domain bitcointoyou.com except for third parties (customers or suppliers) directly involved in the subject matter.

Information classified as SECRET must not be stored or transmitted by simple email. Therefore, it is mandatory the use of strong encryption for additional message content protection and its annexes.

PASSWORD ACCESS

The password for access to computing resources of Bitcoin To You is the responsibility of the employee who should not, under any circumstances, share or lend to other employees and third parties.

Users should use passwords "strong", mixing letters and numbers in all corporate systems and the recommended minimum size for passwords is eight (8) characters.

Information classified as SECRET must be submitted in a long sequence of at least 18 characters, or choose to use a least 1024 bits by the specific key (always using an additional password to protect the encryption key).

Every action done inside or outside the computer of Bitcoin To You environment, the developer's responsibility to be associated with the access credentials associated with actions.

INACTIVE ACCOUNTS

Any access credential that has no activity within 90 days will be blocked for ALL enterprise systems.

MULTI FACTOR AUTHENTICATION (TWO FACTORS)

It is mandatory the use of multi-factor authentication (2FA or MFA, Two factor Authentication or Multi-Factor Authentication) for all services where the option is available.

REMOTE ACCESS

previously registered employees by explicit approval of their direct managers can gain remote access to the computer environment of Bitcoin To You. To do so, complete the form it is necessary that indicates the initial term and final access, your needs and levels of external access . This process should use enterprise equipment provided by Bitcoin To You with the implementation of existing security controls. The connection is made through private corporate VPN.

DOCUMENTS ON DESK

All employees must obey the rules of cleaning and organization of the work environment in order not to unnecessarily expose classified information.

Printed notes and documents that need to be in a paper (printed or notes) should remain the tables on a temporary basis and should be collected in closed rooms

available in your department or any branch of the company that provides security and protection to these materials.

All information must remain the tables can and must be destroyed by the responsible employee or any other person who so want to do it by exercising good information protection practices of Bitcoin To You.

The notoriously orphans important documents (which have signatures for example) shall be deposited in a special cabinet mouth type of wolf so they can be reviewed later before its destruction - safe orphans documents located next to the printers.

This rule applies to the work environment, including workstation, desk, drawers, files and trash.

DEVICE FOR BLOCKING INATIVIDADDE

All corporate device access to enterprise systems must undergo automatic lock after 10 minutes of inactivity (computers, smartphones, tablets or any other device, mobile or not).

TRAFFIC CATCH THE NETWORK

It is forbidden to capture network traffic within the corporate network Bitcoin To You saved events duly authorized by the Security Committee or the safety manager for the sole purpose of diagnosis, auditing and monitoring previously authorized.

PERSONAL DEVICES

The use of personal devices is restricted to guest network / guest of Bitcoin To You.

It is not allowed the connection of non-corporate devices internal networks, wired or wireless.

To employees who need to make use of mobile devices to perform specific functions and tasks, will make using equipment provided by the company, with appropriate controls and protections techniques applied.

SOCIAL NETWORKS

It is forbidden to any employee issue any statement, opinion or comment on behalf of Bitcoin To You without expression approval and alignment with the area of marketing and communication.

The response interactions, reply to comments made by others about the company and the like, can only be made by specific areas of communication and management of social media.

The publication of photos indoors area should also be avoided to prevent restricted information contained in the internal areas of the company inadvertently published.

SOFTWARE APPS AND PLUGINS

It is not allowed to install software not approved by IT and Security area on any devices accessing the information systems of Bitcoin To You which includes: computers, notebooks, and portable devices such as tablets and mobile phones. Including software, applications, free or paid plugins.

The IT and Security area already has a portfolio of tools and applications to meet the business demands including productivity tools and the like.

Most of these tools are already pre-installed on all corporate devices.

ATTITUDE PRIVACY GENERAL

All access to internal systems should have to justify a real business purpose.

It is forbidden access to any information from customers, employees or any record in the information systems of Bitcoin To You without a clear business purpose, and directly linked to the performance of assigned functions in the working relationship between the employee and the company.

It is forbidden the access to customer data out of curiosity.

Like for example:

Access accounts celebrities, public persons, relatives, friends or any other customer without a business purpose and foremost a call related to the case. If you need to solve a problem on their own, such as approving a deposit, open a call and ask a colleague make the approval for you.

MONITORING

The Bitcoin To You reserves the right to monitor all the activities done by their employees in their information systems to ensure compliance with this and other company policies.

The indoors of Bitcoin To You may also suffer audiovisual recording with the main purpose of increasing the security of the internal perimeter of the company against security incidents of any kind.

ACCESS TO THE OFFICE AND ESCORT OF VISITORS

Access to our offices NO can be done by people UNATTENDED. An employee should always escort the visitor SINCE the arrival at the reception of the building to the entrance at the office.

The reception should NOT open the access door, or who has not registered biometrics, will always have to be escorted by another employee. For employees or external consultants who work more than two days a week in the office, we will register your biometrics and free access without escort.

The main door must always be closed, even for quick office outputs (put debris and waste in the floor compartment, for example). Before opening the door, always carefully OBSERVE WHO is in the hall of the elevators on the outside of the office. If there is presence of foreign NOT open the door, return receipt and wait a few minutes before returning to the floor. If necessary building safety to ask to take the floor, checking and escort the person to the correct floor (it may just be another company and have come down on the wrong floor;)

The key points in this chapter are:

- INTERNAL reception should not open the door to give access to the office;
- All visitors should be escorted SINCE the reception of the building;
- we do not allow to rise visitors to our walk without escort of an employee;
- We do not serve customers Bitcoin To You in our office;
- Only open the door after verifying that strangers are not on the floor

AUDIOVISUAL CONTENT RECORDING IN FACILITIES COMPANY

Eventually the business areas, led by marketing can make audio and video recordings inside the company premises. This session brings some recommendations and obligation to be observed during these events:

a) The professionals who will capture the content when they are not direct employees of the company should be under direct supervision throughout their stay in the company least one employee;
b) The contractor and any suppliers, must have a signed NDA and the current BEFORE carrying out the work;

c) The developer and area of work client, will be responsible for compliance with any confidential information such as screens, documents, notes (including the boxes located on the walls used for notes by the teams) ensuring that such information is not captured by photos or videos made within our addictions. The supplier also must review and overshadow any content that is observed during the editing of material and contracting area should always review the final version of the audiovisual production to ensure that confidential information is not accidentally have been captured in the images.

X - Final Provisions

Violation of this policy may result in administrative and / or legal, including the employment contract termination and / or any other relationship contract of service between the employee, associate, consultant and / or partner, as well as any entity with direct or indirect contractual relationship with the Bitcoin to You.