PRIVACY POLICY - NXT

When you access or use services provided by **NXTPAY, NXTBNK, NXT GROUP, NXTGRP, nxtbnk.com (together, "NXT")**, including of, but not limited to, **NXT** account, websites, webapps, Application Programming, mobile apps, smartwatch apps, Interface, products, card processing and card issuing (together and separately, the "Services"), you agree to be bound by this Privacy Policy (together, "Policy").

1. Objective

This Policy was created to ensure the protection, privacy, integrity, disponibility and confidentiality of the data and information under the **NXT** Services.

2. Responsibility

This Policy is the responsibility of **NXT** Technology Department and **NXT** Compliance Department. Any changes to this Policy must be approved by the Technology Department and the Compliance Department of **NXT**. Senior management of both teams are committed to the continuous improvement of procedures related to information, data and cybersecurity.

3. Time Period

This Policy takes effect immediately but may be reviewed annually or when necessary, such as changes in the standards of the Technology Department and the Compliance Department of **NXT**. It could also change whenever information security, guidelines, business objectives, or as required by local regulators.

4. What is Privacy and Data Security

We consider information assets to be the most important assets in the financial market and, therefore, handling them responsibly is our commitment. We are based on the principles of information security, whose objectives are the preservation of the ownership of information, notably its confidentiality, integrity, and

availability, allowing controlled use and sharing, as well as monitoring and handling of incidents arising from cyberattacks.

Confidentiality: Ensuring that the information handled is exclusively known to authorized personnel.

Integrity: Ensuring that information is maintained intact, without undue modifications – accidental or intentional.

Availability: Ensuring that information is available to all authorized persons who handle it.

5. Confidential information

Access to confidential information, including personal data, collected and stored by **NXT** is restricted to professionals authorized to use such information directly and necessary to provide our services. The use of this information for other tasks is limited.

NXT may disclose confidential information in the following cases:

- Whenever required by law, competent authority, court order, or judicial mandate;
- To credit protection and defense bodies and service providers authorized by **NXT** to defend its rights and credits;
- To financial market regulators
- To its banking partners, card issuing partners, card processing partners, credit partners or other partners which ensure the availability of our Services; and
- To other financial institutions, provided it is within the legal parameters established for this purpose. In this case, the user may cancel their authorization at any time.

6. General treatment

A. Information Treatment

Information under the custody of NXT, even if belonging to customers or suppliers, must be protected against unauthorized access. The generation, use, storage, maintenance, distribution, and destruction of information must be done according to the company's needs, and these processes must be properly documented.

The information must be stored for the time determined by NXT, and be in a retrievable file format to be extracted when necessary. The location of information storage must be appropriate and protected against accidents and unauthorized access.

B. Access to Information

The use of external communication networks (Internet, private networks, etc.) must be controlled through Firewalls Servers, Internet Access Servers, AntiSpam Servers, Antivirus Tools, and operating system policies that guarantee that only necessary resources are available for work without risks to the operating environment.

External access to the organization's systems, when carried out by the Technical Support Area staff or service providers, must be controlled and restricted to the necessary services, keeping usage logs and restricting to the minimum necessary. The solution found for each case must be formalized and documented. The organization data will only be sended, either to meet business requirements or to facilitate the resolution of problems, also must be evaluated based on risks and by adopting procedures that guarantee the control and integrity of data, in addition to the legitimacy of the recipient of the information. What is agreed upon must be formalized and approved by the managers responsible for the information.

C. Application Systems

Application systems developed within the organization must be documented and controlled regarding changes or corrections made, with logs of what was done

and secure storage of the source library. All necessary information for eventual reconstruction of the applications must be included in their documentation. Application systems developed outside the organization, owned by third parties (with a usage license for the organization), must have the source and additional resource library (acquired libraries, components, etc.) under the custody of a reputable entity, agreed upon between the organization and the software provider company. Such sources must always be updated and verified for their validity and synchronization with the version in use in the production environment.

7. Cyber security and information management

The management of security controls aims to ensure that operational procedures are developed, implemented, and maintained or modified in accordance with the objectives set in this Policy.

7.1 Information Access Management

Access to information is controlled, monitored, restricted to the least privilege and permissions possible, periodically reviewed, and promptly canceled at the end of the employee or service provider's contract. Critical or sensitive information processing equipment and facilities are kept in secure areas with appropriate access control levels, including protection against physical and environmental threats. **NXT** employees and third parties are periodically trained on information security concepts through an effective cybersecurity awareness and culture dissemination program.

7.2 Environment Protection

Controls and responsibilities are established for the management and operation of information processing resources, willing to guarantee security in the technological infrastructure through effective management in monitoring, treatment, and response to incidents, with the purpose of minimizing the risk of failure.

7.2.1 Authentication

Access to information and technological environments of CirfraPay must be allowed only to people authorized by the Information Owner, taking into account the principle of least privilege, segregation of conflicting functions, and information classification. Access control to systems must be formalized and must include, at a minimum, the following controls:

- The use of individualized identifiers (access credentials), monitored, and subject to blocking and restrictions (automated and manual);
- The removal of authorizations granted to users who have been removed or dismissed from **NXT** or have changed functions; and
- The periodic review of granted authorizations.

7.2.2 Information Security Incident Management

The behavior of possible attacks is identified through detection controls implemented in the environment, such as content filters, malicious behavior detection tools, antivirus, antispam, among others.

7.2.3 Information Leakage Prevention

NXT uses control for data loss prevention, responsible for ensuring that confidential data is not lost, stolen, misused, or leaked on the web by unauthorized users.

7.2.4 Intrusion Tests

Internal and external intrusion tests on network and application layers must be performed at least annually.

7.2.5 Vulnerability Scanning

Internal and external network scans must be performed periodically. Identified vulnerabilities must be treated and prioritized according to their level of criticality.

7.2.6 Malicious Software Control

All assets (computers, servers, etc.) that are connected to the corporate network or use information from **NXT** must, whenever compatible, be protected with an anti-malware solution determined by the Information Security area.

7.2.7 Cryptography

All cryptography solutions used in **NXT** must follow the Information Security rules and security standards of regulatory agencies.

7.2.8 Traceability

Automated audit trails must be deployed for all system components to reconstruct the following events:

- User authentication (valid and invalid attempts);
- Access to information;
- Actions performed by users, including creating or removing system objects.

7.2.9 Network Segmentation

- Computers connected to the corporate network must not be directly accessible from the Internet;
- Direct connection of third-party networks using remote control protocols to servers connected directly to the corporate network is not allowed;

7.3 Business continuity

The business continuity process is implemented to reduce the impacts and losses of information assets after a critical incident to an acceptable level, through the mapping of critical processes, analysis of business impact, and periodic disaster recovery testing. This process includes business continuity related to cloud-based services and testing for cyber attack scenarios.

8. Safety guidelines for employees, customers and users

8.1 AUTHENTICATION AND PASSWORD

Recommendations for information handling for customers: The customer is responsible for the actions executed with their identifier (login/username), which is unique and accompanied by an exclusive password for individual identification/authentication when accessing information and technology resources. We recommend that:

- Keep confidentiality, memorize, and not record the password anywhere. In other words, do not tell anyone and do not write it down on paper;
- Change the password whenever there is any suspicion of compromise;
- Create quality passwords that are complex and difficult to guess;
- Prevent the use of your equipment by other people while it is connected/logged in with your identification;
- Always lock the equipment when absent.
- Whenever possible, enable a second factor of authentication (e.g., SMS, Token, etc.).

Recommendations for information handling for employees: The person who receives information inappropriately should immediately contact the sender and alert them to the mistake. Information available on the Internet should only be accessed for the purpose of executing activities exclusively of interest to the company.

All information on paper, removable media, or any other storage medium should be destroyed after use or stored in a way that is not available to unauthorized

persons. Maintenance on equipment that stores information should be accompanied by a representative from the area whenever that equipment is in use or logged in with the credentials of the employee who needs support.

When sold, returned to the manufacturer, sent for maintenance, or moved to other users, the information contained must be destroyed before releasing the equipment. Managers must determine the rules for accessing and distributing information, considering the following items:

8.2 ANTIVÍRUS

We recommend that the customer keep an updated antivirus solution installed on the computer used to access the services offered by **NXT**. In addition, keeping the operating system updated with the latest updates is recommended.

8.3 SOCIAL ENGINEERING

Social engineering, in the context of information security, refers to the technique by which one person seeks to persuade another, often by abusing the user's naivety or trust, with the aim of deceiving, scamming, or obtaining confidential information.

8.3.1 PHISHING

Technique used by cybercriminals to deceive users through the sending of malicious emails, in order to obtain personal information such as passwords, credit card information, social security number, bank account numbers, among others. Phishing emails can be approached in the following ways:

- When they seek to attract users' attention, either by the possibility of obtaining some financial advantage, by curiosity or by charity;

- When they try to pass themselves off as official communication from well-known institutions such as banks, e-commerce stores, among other popular sites;
- When they try to induce users to fill out forms with their personal and/or financial data, or even to install malicious software that aims to collect sensitive information from users.

8.3.2 SPAM

These are unsolicited emails, which are usually sent to many people, typically with advertising content. In addition, Spam is directly associated with security attacks, being one of the main responsible for the propagation of malware and phishing attempts.

8.3.3 FALSE TELEPHONE CONTACT

These are techniques used by fraudsters to obtain information such as personal data, passwords, tokens, cell phone device identification code (IMEI), or any other type of information for the purpose of fraud.

9. Questions and Report

Any indications of irregularities in compliance with the provisions of this Policy will be subject to internal investigation and should be immediately reported to our customer service channels.

10. Contact

Internet Banking: login, access password, and security key or confirmation of customer's personal knowledge information.

Website: Fulfilling the form available in nxtbnk.com

11. Update history

Policy created on 01, September 2024.