Corporate Cybersecurity Policy

Executive Summary

This Policyestablishes the guidelines to compose a complete and consistent information security and cyber risks program, aiming to comply with the provisions of CMN Resolution No. 4,893 and BCB Resolution No. 85 of the Central Bank of Brazil.

Corporate Cybersecurity Policy

INDEX

1. GOAL

Establish guidelines to compose a complete and consistent information security and cyber risks program, aiming to:

a) Protect the value and reputation of the company;
b) Guarantee the confidentiality, integrity and availability of the Travelex Confidence Group's information, and third-party information held by it, against undue access and unauthorized modifications, also ensuring that the information will be available to all authorized parties, when necessary;
c) Identify Cyber Security violations, establishing systematic actions to detect, treat and prevent incidents, threats and vulnerabilities in physical and logical environments, aiming to mitigate cyber risks, among others;
d) Ensure business continuity by protecting critical processes from unacceptable disruptions caused by significant failures or disasters;
e) Meet legal, regulatory requirements and contractual obligations relevant to the company's activity;
f) Raise awareness, educate and train employees through the Corporate Cybersecurity Policy, internal standards and procedures applicable to their daily activities;
g) Establish and continually improve a Cybersecurity Risk Management process.

2. SCOPE AND APPLICABILITY

This Policy covers aspects related to information security and controls over Cyber Risks, involving technologies, processes, people and physical facilities, being applied to all areas, employees and service providers of the companies in the Travelex Confidence Group, formed by Travelex Banco de Câmbio SA and Confidence Corretora de Câmbio SA ("Travelex Confidence Group").

3. CONCEPTS

Cyber Security consists of preserving the properties of information, notably its confidentiality, integrity and availability, allowing the use and sharing of information in a controlled manner, as well as monitoring and handling incidents arising from cyber-attacks.

Confidentiality:guarantee that information is accessible only to authorized people.
Integrity:safeguarding the accuracy and completeness of information and processing methods.
Availability:ensuring that authorized users gain access to information and corresponding assets whenever necessary.

Cyber Risks: Risks of cyber-attacks, arising from malware, social engineering techniques, invasions, network attacks (DDoS and Botnets, ransomware), external fraud, unprotecting the company's data, networks and systems, causing considerable financial and reputational damage.

Malware:

a) Virus:software that causes damage to the machine, network, software and database;
b) Trojan Horse:appears inside other software and creates a door for computer invasion;
c) Spyware:malicious software to collect and monitor usage information;
d) Ransomware: Malicious software that blocks access to systems and databases, requesting a ransom for access to be reestablished.

Social engineering:

a) Pharming: directs the user to a fraudulent website, without their knowledge;
b) Phishing:links transmitted by e-mail, pretending to be a trusted person or company sending official electronic communication to obtain confidential information;
c) Vishing:pretends to be a trustworthy person or company and, through telephone calls, tries to obtain confidential information;
d) Smishing:pretends to be a trustworthy person or company and, through text messages, tries to obtain confidential information;
e) Personal access:people located in public places such as bars, cafes and restaurants who capture any type of information that could later be used for an attack.

External fraud and intrusions: Carrying out operations by fraudsters, using attacks on bank accounts, using knowledge and tools to detect and exploit specific weaknesses in a technological environment.

DDoS Attacks and Botnets: Attacks aimed at denying or delaying access to the institution's services or systems; In the case of Botnets, the attack comes from a large number of infected computers used to create and send spam or viruses, or flood a network with messages resulting in denial of services.

4. PRINCIPLES

The protection and privacy of customer data reflect the values of the Travelex Confidence Group and reaffirm its commitment to continually improving the effectiveness of the Data Protection process.

Regarding our customers' information, the following provisions are complied with:

a) They are collected ethically and legally, for specific and duly informed purposes;
b) They will only be accessed by people authorized and qualified for their proper use;
c) They may be made available to companies contracted to provide services, with such organizations being required to comply with our data security and privacy guidelines;
d) The information contained in our records, as well as other requests that may guarantee legal or contractual rights, will only be provided to interested parties, upon formal request, following current legal requirements.

5. CORPORATE GUIDELINES

Compliance with the Corporate Cybersecurity Policy is the responsibility of all employees and service providers, who must comply with the following guidelines:

a) Protect information against unauthorized access, modification, destruction or disclosure;
b) Provide the appropriate classification of information, under the criteria of confidentiality, availability and integrity;
c) Ensure that the resources used to perform their role are only used for purposes approved by the Travelex Confidence Group;
d) Ensure that the systems and information under its responsibility are adequately protected;
e) Ensure the continuity of processing of critical business information;
f) Comply with the laws that regulate the activities of the Travelex Confidence Group and its operating market;
g) Select information security mechanisms, balancing risk, technology and cost factors;
h) Immediately report any non-compliance with the Corporate Cybersecurity Policy to the Cybersecurity area.

6. MANAGEMENT STRUCTURE

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

6.1 Management of access to information

Created network users, as well as computers connected to the network, are authorized, authenticated and identified by the Active Directory (Microsoft) structured database service, which stores information about network objects (user accounts, service accounts, computers , email and security groups).

The Cyber Security team is responsible for the process of creating and deactivating network access logins, even if the process is carried out by another operational area (for example IT), and can only deactivate the login of a Travelex Confidence Group employee, after confirmation of dismissal by HR or through a formal request from the employee's immediate or immediate manager.

To create logins for service providers (third parties), the request must come from the manager responsible for the project where the service provider will be located. The responsible manager must inform Cyber Security every month of the end of each provider's work, so that their network login can be deactivated.

Passwords for users of systems, databases and networks are individual, confidential and non-transferable and must not be disclosed under any circumstances. The user is responsible for keeping their password confidential, monitoring their account and immediately communicating to the Help Desk team if they suspect it has been compromised.

Access to information in systems and databases of the Travelex Confidence Group is controlled, monitored, restricted to the lowest possible permission and privileges, periodically reviewed with the approval of the person responsible and information manager, as well as canceled in a timely manner at the end of the contract. of the employee or service provider.

The rules for granting and periodically reviewing access are applied to all systems controlled by the Cybersecurity area and all systems that require the creation of a login in the database for direct access.

6.2 Use of Email and Web Browsing

Each user is responsible for the content stored and sent through their email account.

The Travelex Confidence Group reserves the right to monitor and interfere with message traffic, with the purpose of verifying compliance with security standards, whenever it deems necessary.

The sending or forwarding of "chain letters" and "spam" type messages is prohibited. The use of company lists and/or address books for the distribution of messages that are not of strict functional interest and without due permission from the person responsible for the lists and/or address books in question is prohibited.

Confidential information should not, under any circumstances, be sent by electronic mail without some form of protection against leakage and alteration.

Access to corporate email via cell phone will only be permitted after approval by the Cybersecurity area.

All internet access is carried out through an appropriate filter that restricts access to websites not permitted by the Cyber Security area.

All internet access made by users is subject to monitoring.

Granting access to blocked websites will only be carried out after analysis and approval by the Cybersecurity area.

6.3 Control over the use of administrative privileges

Rules are established to standardize and regulate the use of accounts with administrative privileges (domain administrators, local administrator, database administrator, system user).

Administrative privilege for an account can only be granted upon analysis and approval by the Cybersecurity area.

Company employees who have administrator privileges will only be able to access locally or remotely the stations/servers that have been designated for their responsibility.

For local or remote access to stations/servers, the employee must only connect using their own network login. The use of "service accounts" to log into servers is not permitted.

Service accounts that have domain administrator privileges must have dual custody of the password, between the responsible area and Cyber Security.

It is expressly prohibited to create network logins or service accounts without authorization from the Cybersecurity area, as well as deactivate, pause or turn off any information security and traceability monitoring feature, including access and audit logs, except with formal authorization from the Cybersecurity area.

6.4 Classification

a) Information

The Travelex Confidence Group establishes the information classification process to support the determination of needs, priorities and level of security when processing company information, covering its entire life cycle and in any storage or communication medium.

Classification and associated protection controls for information must take into account business needs for sharing or restricting information as well as legal requirements. Assets other than information assets should also be classified according to the classification of information stored, processed, handled or protected by the asset.

All company information must have a designated owner. The owner of information is a person who has authorized responsibility for controlling its creation, assignment of rights, storage, transportation, use, retention and disposal. The term owner does not mean that the person actually has any ownership rights to the information.

All information must be identified and must have a responsible owner, who will be responsible for determining its classification, as well as carrying out critical analysis. The information owner may define additional security controls, if deemed necessary.

The Travelex Confidence Group establishes 4 (four) categories for classifying Information (Confidential, Restricted, Personal Data and Public), which are based on the criteria of Confidentiality, Integrity and Availability.

Confidential	This is data that can cause a significant level of risk and impact to the organization, its affiliates or customers if such information is improperly accessed, lost, altered or made public in any way.
Restricted	Restricted data means non-personal information that is not approved for general circulation outside the organization, where unauthorized disclosure, alteration or destruction of the data could result in a moderate level of risk or impact to the organization, its affiliates or customers. It must not be seen or accessible to external parties unless approved by the Data Owner.
Personal data	Information that allows you to identify, directly or indirectly, an individual as Name, ID, CPF, gender, date and place of birth, telephone number, home address, location, photograph, bank card details, income, among others.
Public	Public data is public domain information that has been approved for external communication where disclosure, alteration or destruction of data would result in little or no risk to the organization, its affiliates or customers.

b) Assessment of the relevance of incidents

Cybersecurity incidents will be evaluated and treated according to specific procedures, the relevance of which must be prioritized based on the criticality of the services, combined with the analysis of the compromise of confidentiality, integrity and availability of information.

6.5 Inventory and asset control (hardware and software)

All internal assets associated with information and with information processing resources must be identified, have a person responsible, maintained in a repository with periodic review, as well as the classification of information on the identified asset.

Any and all acquisitions of new software or services, including cloud storage and computing, must first be analyzed by the Cybersecurity area, in order to determine the baseline requirements for information security and cyber risks.

6.6 Secure configuration of hardware and software on mobile devices, desktops and servers

Procedures are defined for applying security updates to the operating systems of servers and stations, as well as updating versions of security and network infrastructure equipment, with the aim of preventing and/or responding to security incidents.

Rules must be established to specify the minimum configuration requirements for servers and workstations, aiming to guarantee information security.

a) Secure server configuration

The location where the Travelex Confidence Group's servers are located must have physical security control regarding location, cabling, temperature control, electrical network and fire fighting. Access must be restricted to administrators and authorized people. The entry and exit of people who do not belong to critical environments must be recorded and archived to allow periodic audits.

Server administration must be carried out through sessions authenticated by username and passwords.

Remote access to the server must be carried out using tools approved by the Cybersecurity area and restricted to machines that perform this function in the management network.

The server must have its log system and/or alerts enabled. Logs should not be deleted without authorization from the Cybersecurity area.

The use of the server is restricted to activities related to the Travelex Confidence Group's business/services, in order to maintain high levels of productivity, availability and technological and security updates.

Mechanisms for monitoring memory, disk capacity and communication with the network and security must be applied, with the aim of preventing and responding to incidents.

Any configuration change must be evaluated, approved, approved and documented by the IT area.

b) Secure desktop configuration (workstations)

The physical installation of workstations must be carried out exclusively by the IT department or by formally authorized companies.

The cabinet (CPU) should only be opened by an authorized person for maintenance or updating. All stations must have Travelex Confidence Group asset identification.

Local workstation administrators must be analysts from the IT support team, domain administrators or people authorized by the Cyber Security area and the requesting management.

All workstations must receive and correctly apply Active Directory group policies (GPO), approved by the IT and Cybersecurity area and only applied by the IT area. In case of exception, a local policy must be applied to each station, following the domain standard.

c) Secure notebook setup

The use of the mobile computer is restricted to activities related to the Travelex Confidence Group's business/services.

The user of the mobile computer must sign the Mobile Computer Custody Agreement, declaring themselves responsible for the equipment and its data.

The mobile computer must have a Travelex Confidence Group asset identification label.

For mobile computers of employees who frequently use the equipment in an external environment, the hard disk encryption mechanism must be applied to protect information.

A local firewall system must be applied to filter packets on the wireless interface.

The installation of antivirus software other than that provided and configured by the IT area of the Travelex Confidence Group is prohibited.

Corporate antivirus software must always be updated to the latest version available. Under no circumstances may the notebook's antivirus service be interrupted.

Internet connection sharing, via wireless, must be blocked.

6.7 Network Communications Control

a) Classification of zones

Networks must be classified into four trust zones that reflect the levels of control applied to the network segment, systems and platforms connected to them:

i. *Unreliable*– must cover all systems and services not controlled by the company, including business partners and public networks;

ii. *Intermediate*– must cover all networks and devices used to interact with the untrusted environment, including DMZ and publicly accessible servers;

iii. *Reliable*– all internal networks (LAN/MAN), as well as non-critical servers and internal user desktops must be considered in this zone;

iv. *Restricted*– must cover highly critical systems/servers for the company's business.

b) Communications control

Network and inter-zone communications must be controlled by security control devices (firewalls, Proxy servers, packet filters and VPN concentrators) positioned on the border between them, in order to carry out adequate control.

Firewalls must be hybrid devices capable of performing communications control based on deep packet inspection applied to communication between the Untrusted and Intermediate Zones, as well as serving as a Proxy for applications for communication between the Intermediate and Trusted zones.

Communications control rules must be applied in the following cases:

i. Partners accessing company applications through VPN;
ii. Remote Partners/Users/Employees accessing services through a WEB interface from a browser;
iii. Remote employees accessing company applications through VPN (Virtual Private Network) via a device governed by the IT area. In this case, user authentication must be carried out so that access is granted;
iv. Visitors and employees accessing the Internet from devices not governed by IT within the buffer zone;
v. Employees accessing the internet from the trusted zone;
vi. Communication between internal and external utility services, such as DNS and SMTP;
vii. Access to public services from clients and/or networks not governed by the company's IT;
viii. Internal communications to the trust zone;
ix. Communications between the trusted zone and restricted zone systems and services.
x. New connections to the network infrastructure must be previously evaluated by the Cybersecurity and Infra IT areas, under the aspects of security and availability.

c) Rules for wireless network connections

Wireless connections (Wi-Fi) must only be allowed through Access Points (AP), and any other type of wireless connection must be blocked, including point-to-point (Ad hoc) connections.

Access points must be managed using protocols that use encryption when transferring data over the network, such as SSH and SSL.

It is necessary to generate audit trails of user and administrator access and configuration changes.

There must be a process for automatic detection of unauthorized access points (Rogue Access Point) and point-to-point wireless connections (Ad-hoc).

Only the WPA2 protocol should be used for wireless connections

Mobile devices belonging to third parties or employees' private devices may only use the guest network; under no circumstances will this type of equipment be connected to the corporate network.

There must be a device compliance verification process before it joins the wireless network. This process must be auditable and generate confirmation logs or reports.

Exceptions must be submitted for Cyber Security review and approval.

d) Secure configuration of hardware and software on mobile devices, desktops and servers

The use of recording devices via USB/CDR/DVDR is not permitted.

6.8 Environmental protection

Controls and responsibilities are established for the management and operation of information processing resources that guarantee security in the technological infrastructure of local networks and the internet, through monitoring, treatment and responses to incidents, to minimize the risk of failures and secure network administration of communications.

a) Firewall management and rules

Travelex Confidence Group firewalls must have the log system and/or alerts enabled. The messages generated must be correlated and receive critical analysis by the team that manages the equipment.

Firewall management must be carried out using protocols that use encryption when transferring data over the network, such as SSH and SSL.

Firewall administrators must subscribe to or constantly check the equipment manufacturer's vulnerability bulletins. Other sources of information are also recommended.

All firewall rule maintenance (creation, change and deletion of rules) must be approved by the Cybersecurity area.

Every physical installation of firewall equipment must first go through a Change Management process, providing for the rollback procedure.

Firewalls must be maintained in secure areas, protected by a defined security perimeter, with appropriate security barriers and effective access control. These areas must be physically protected from unauthorized access, damage or interference.

b) Threat and vulnerability monitoring

The Travelex Confidence Group's threat and vulnerability monitoring process covers detected and prevented intrusions, protecting the network from malicious activities such as: SQL injections, cross-site scripting, buffer overflows, etc.

Also part of the monitoring are threats related to viruses, Trojans, worms, spyware and rogueware, preventing them from affecting the network and other devices, as well as Botnet and APT Zero Day attacks, which are known threats (attacks). by reaching a network of computers, infecting them with malicious software that can be controlled remotely, forcing them to send spam, spread viruses or carry out DDoS attacks, without the knowledge or consent of their "owners".

Internet access is controlled and managed through web filter policies, blocking navigation to web addresses that present security risks. Exceptions are released through prior analysis by the Cybersecurity area, upon approval by the Board responsible for the request.

Any incident related to threats/effective attacks in the environment must be recorded and treated through the Incident Registration and Response process, containing root cause analysis, specific solution, definitive solution, operational impact, financial impact and risk classification.

c) Infrastructure Monitoring

The IT area monitors Servers and Links with alerts on the computer screen, on television in the area, as well as alerts via cell phone.

In relation to the physical stores of the Travelex Confidence Group, internal monitoring is carried out regarding unavailability and latency of links. By analyzing behavior, a possible attack can be identified.

Any incident related to the unavailability and latency of servers and links must be recorded and treated through the Incident Registration and Response process, containing root cause analysis, specific solution, definitive solution, operational impact, financial impact and risk classification.

d) Audit trails and monitoring

Any information that is produced, transmitted, processed or stored is subject to monitoring and auditing, therefore, the Travelex Confidence Group, in full legal compliance, reserves the right to monitor and record all access to it.

The generation of audit trail records (log) must be synchronized with an eligible reliable clock on the network. All records must be time stamped in the same format, synchronized with a master clock.

e) Update security and antivirus patches

The IT area is responsible for maintaining a routine for identifying and monitoring updates to operating systems, antivirus and versions (firmware) of network and security equipment.

For critical updates, an approval environment must be prepared to receive and test the new updates, before installing them on equipment (desktops, servers, firewalls, etc.).

Necessary updates that cannot be applied, due to any impossibility in the environment, must be communicated to the Cybersecurity area.**Security Tests (Pentest)**

The Cybersecurity area periodically carries out penetration tests in the technological and network environment, to evaluate the system's activities, involving the search for potential vulnerabilities, hardware/software failures, operating system deficiencies, internet publishing components, among others. An assessment of the impact on identified gaps and diligence with the areas responsible for due treatment and technical solution is applied.

6.9 Record management and incident handling

Record management and incident handling is the responsibility of the IT, Operational Risk and Cybersecurity areas of the Travelex Confidence Group.

Identified incidents must be recorded by all company employees, through a system made available for this purpose.

When opening an incident, the type of incident that occurred must be mentioned, as detailed below, but not limited to:

a) **Cybersecurity/Information Failure:** sensitive/confidential information available without restriction; password sharing; unauthorized access, cyber attack, malware, etc.;
b) **Failure or Error in systems:** system with error message; system performing wrong calculation, system crashed, etc.;
c) **Unavailability:** internet link drop; unavailable telephone line; lack of electricity, etc.;
d) **Slow:** network, database, systems showing excessive slowness, etc.;
e) **Operational failure:** process not executed correctly and/or defined, etc.;
f) **Frauds:** atypical operations that denote fraud.

The report of the event (incident) must be very detailed in order to provide sufficient information for the investigation and appropriate treatment.

Depending on the type of incident, the record will be directed to the corresponding team responsible for handling and responding to the incident, which must detail the root cause, the specific solution, the definitive solution, action plan and deadline, to avoid recurrence and the operational impact. For the purposes of BCB resolution 4,893 and BCB resolution 85 Art. 3º, V, "b", for service providers whose provision involves access to personal data, that is, incident to the LGPD, the conclusion of the term of use will be determined (DPA), which deals with data processing.

This management scope considers the scope of information received from Travelex Confidence Group service providers.

Incidents classified as "Critical" risk must be presented to the Travelex Confidence Group Risk Management Committee, which will decide on sharing information about relevant incidents with other institutions and making it available to the Regulatory Body.

Before the Central Bank of Brazil (Regulatory Body), the Director responsible for the Cybersecurity Policy must be appointed, as well as for carrying out the incident response process.

Annually, with a base date of 12/31, a report on incident management for the period must be issued and made available to the Regulatory Body.

6.10 Business Continuity

The business continuity management process, relating to information security, must be implemented to minimize impacts and recover losses of information assets, after a critical incident, to an acceptable level, through the combination of requirements such as operations, key employees , mapping critical processes, business impact analysis and periodic disaster recovery testing. This process includes business continuity related to contracted cloud services and tests planned for cyber attack scenarios.

The management process of the Travelex Confidence Group's Business Continuity Plan covers the Business Impact Analysis (BIA-PCN) of the company's critical areas, conducted by the Cybersecurity area, through which the inventory of critical processes is carried out, the time required to return to operation in the event of an incident and activation of the contingency, the interdependence of processes and systems, the key people who will be activated in the event of the activation of the contingency and the financial, operational, regulatory and image impacts. The BIA must be reviewed annually.

Periodic (annual) tests are conducted by the IT area, according to predicted incident scenarios, such as the unavailability of the technological environment and building abandonment, with the aim of assessing the effectiveness of the contingency environment planned for critical processes and systems .

6.11 Backups of data and information

The IT area is responsible for maintaining the backup process for the Travelex Confidence Group's critical information.

This process consists of backup to disk, using the data duplication technique, which aims to analyze, identify and remove duplication in data, thus reducing the amount of information to be stored.

Backups of File Servers and network folders containing database backups are performed.

The IT team is responsible for checking, on a daily basis, the execution of backups carried out.

6.12 Secure Software Acquisition, Development and Maintenance

Information security aspects are involved in the following phases of the Software Acquisition, Development and Maintenance Cycle, namely:

a) Conceptualization and Planning
b) Analysis and Design
c) Construction and Development
d) homologation
e) Implantation

a) Safe Development Environment

There must be formal and documented procedures that detail the Development Cycle with the necessary approvals required for each migration between the above-mentioned phases.

IT Management must follow the formal and documented process, aiming to ensure that the integrity of the software is preserved through version control and changes made to the product. This process must be formalized in the methodology that supports the Travelex Confidence Group Development Cycle.

The process and product quality assurance process must be maintained to determine the existence of problems and defects in all software during its development and maintenance process.

Access to source codes and associated items (such as drawings, specifications, verification and validation plans) of software in production or in the development process must be controlled and restricted to authorized individuals. The nature and content of any information that comprises or results from the professional activities of the Travelex Confidence Group must not be disclosed to third parties.

Administrative measures will be applied in the event of infringements relating to the disclosure to third parties of information relevant to the development of the project.

b) Conceptualization and Planning Phase

The description of information security requirements should be part of the requirements gathering process phase. These requirements must be included in project requirements documents, with the aim of assigning security controls to the software in a balanced way from the beginning of its life cycle and identifying the most appropriate security features to ensure the necessary level of security for the information processed. by the software.

The Cybersecurity area must be involved in the approval of these security requirements.

The information processed, presented, transmitted and stored by the software must be identified and classified (if not already) during its design in terms of security requirements, according to item 6.3 of this Policy.

The client (requester) must formally accept the proposed controls, the existing risk of not implementing the controls or register their commitment to implement them in the business process. The important thing is to ensure that you are aware of the existing risks and benefits.

c) Security Tests

There must be a formal, documented process for performing security testing before migrating software from the development environment to production. This process must define who is responsible for carrying out the tests, as well as describe their scope and depth.

Security tests should not use real data, that is, data from production. The tests must be carried out in a segregated environment specifically designed for this purpose, and by a team different from that participating in the system development. Therefore, it is important that the software requirements already contain the information that will make up the security tests so that they can be generated and made available at the appropriate time for carrying out the tests.

Functional security testing is mandatory for all software developed for use by the Travelex Confidence Group. It consists of checking each system security control. Functional testing must therefore consider each item contained in the safety specification.

Functional tests must involve the customer in the Approval phase. If the tests are successful, they will explicitly record their approval.

d) Hiring Third Parties

Software development by third parties must be controlled. The signed contract must specify the methodology used in the stages of the Software Development Cycle, provide for intellectual property issues, confidentiality agreements and include the right of the Travelex Confidence Group to audit the third party, with the aim of ensuring that all requirements described are being met.

e) Software Package

The acquisition of Package Software must follow a formal and documented process of functional assessment (performed by the user area) and technical assessment (performed by the development area). The technical analysis must include the survey of security requirements, specification of functionalities, architectural design and testing, as well as the assessment of Operational Risk criteria and data and information protection.

The contract with the supplier must contain clauses that protect the Travelex Confidence Group from the risks of discontinuing the provision of support and corrective and evolutionary maintenance services, as well as the risks of not meeting legal deadlines for software adjustments.

In the case of Software Packages that automate critical operations of the Travelex Confidence Group, controls must be implemented to protect against the risk of the supplier leaving the market or discontinuing the software, such as adopting a third party acting as custodian of the source code.

Changes to Software Packages must be carried out in a controlled manner by suppliers. Processes must be established that formalize the receipt, change, approval, distribution and storage in a centralized repository of patches and versions of Package Software.

6.13 Third Party Operations

The service providers' contract must necessarily establish that the Corporate Cybersecurity Policy is fully complied with, as well as the security regulations related to the scope of the contract and also establish the penalties resulting from any violation of the defined security rules.

Every service provider must be up to date with the Travelex Confidence Group's security rules and only use services for which they have permission.

Any equipment owned by the service provider is only installed and/or used within the scope of the Travelex Confidence Group, subject to identification and authorization.

The logical accesses of service providers are managed in accordance with item 6.1 of this Policy.

The Travelex Confidence Group may, at any time, monitor, audit and suspend access granted to service providers, regardless of any prior notice or communication.

6.14 Processing, Data Storage and Cloud Computing

According to CMN Resolution No. 4,893 and Resolution 85 of the Central Bank of Brazil, for contracting data processing and storage and cloud computing services, the Travelex Confidence Group must ensure an effective procedure that ensures adherence to the rules set out in regulations in force.

For the purposes of regulatory compliance on the analysis of operational and cyber risks, business continuity, confidentiality, provision of information to the Regulatory Body, Incident Response, among others, the due-diligence process must be considered together with to the supplier of the contracted product or service, prior to the formalization of the service provision contract between the contractor (Travelex Confidence Group) and the contractor (Supplier).

The contracting of relevant processing, data storage and cloud computing services, as well as contractual changes to these services, must be previously communicated to the Central Bank of Brazil, at least sixty days before contracting the services or contractual changes.

6.15 Use of mobile devices

Users are part of the process of protecting the company's network and confidential data that is stored or accessed using a mobile device (cell phone, smartphone, tablet, etc.), and must take the following measures:

a) Do your best to protect your device against loss or theft;

b) Immediately inform IT Infrastructure or Cyber Security of a lost or stolen device;

c) Keeping the operating system and applications up to date and/or checking with IT if you are unsure how to do so;

d) Use only original and approved applications to access company data;

e) Use security programs and practices to prevent piracy and/or tampering with software/security settings on the device;

f) Make sure your device is programmed to lock the screen with a password or PIN if it is idle after five minutes;

g) Pay attention to the handling of information on mobile devices in terms of security and information classification.

6.16 Information Security Awareness and Cyber Risks

The Cyber Security area is responsible for applying procedures on information security awareness and cyber risks for employees and service providers.

The hired employee must complete online training (mandatory) on Information Security.

Awareness and training campaigns containing lectures, periodic information security bulletins, among others, should be intensified as a program in the Cyber Security area, containing mechanisms for measuring the employee training and awareness program.

Clean Table

Paper and removable computer media that contain sensitive or critical information to the Travelex Confidence Group's business, when not in use, must be stored appropriately, preferably in locked drawers or cabinets.

All other non-public information must be kept secure when employees leave the building at the end of their workday.

During working hours, you should avoid leaving the items listed below on the work table without due supervision:

a) Confidential documents with information from customers, partners and competitors.
b) Diaries, sheets of paper, books, pads and notebooks;
c) Removable media (Pen Drivers, external HD, CD and DVD;
d) Keys and Access Cards;
e) Passwords in POST-IT or any other notepad.

Documents must be removed from the printers by those responsible, immediately after printing. Documents found adrift by employees of the Travelex Confidence Group must be delivered to the Cybersecurity area.

7. POLICY VIOLATIONS

The following situations are considered violations of the Corporate Cybersecurity Policy and respective regulations, but are not limited to these:

a) Any actions or situations that may expose the Travelex Confidence Group to financial and image loss, directly or indirectly, potential or real, compromising its information assets;
b) Improper use of corporate data, unauthorized disclosure of information, commercial secrets or other information without the express permission of the information manager;
c) Use of data, information, equipment, software, systems or other technological resources for illicit purposes, which may include violation of laws, internal and external regulations, ethics or requirements of regulatory bodies in the area of activity of the Travelex Confidence Group;
d) Failure to immediately notify the Cybersecurity area of any non-compliance with the Policy.

Signs of irregularities in compliance with the provisions of this policy must be reported immediately to the email addresssegurancacibernetica@travelexbank.com.brand will be subject to internal investigation. If the actual irregularity is ascertained, the Employee will be subject to the penalties applicable by the Travelex Confidence Group (verbal warning, written warning, suspension and dismissal for just cause).

Any exceptions must be evaluated and approved by the Cybersecurity Manager and Legal Director, according to risk analysis, impact and mitigation and acceptability criteria.

8. RESPONSIBILITY

The Senior Management of the Travelex Confidence Group is committed to the continuous improvement of the procedures and controls listed in this Policy, which must be the subject of recurring agendas in the company's internal Committees.

9. REVISION

This policy was reviewed, updated, and approved by the board of directors on May 7, 2024. Subsequent reviews and updates should occur annually or in accordance with process reviews, or adjustments to comply with legal or regulatory requirements.