OBJECTIVE

Present the mandatory information security requirements that must be observed by the CONTRACTED PARTY, considering the processing, transmission and/or storage of information from CLARO customers and employees.

1 REFERENCE DOCUMENTS

For the development of this document, the following were considered:

☒ CLARO Safety Standards;

☒ ABNT NBR ISO/IEC 27002-2013 - Chapter 5 - Relacionamento na Cadeia de Suprimento (Relationship in the Supply Chain);

☒ Law No. 13,709/18 - General Data Protection Law.

2 INFORMATION SECURITY ORGANIZATION

☒ The CONTRACTED PARTY must have an information security management model, to prepare, disseminate and update security policies and guidelines.

☒ The CONTRACTED PARTY shall designate a person responsible for the information security management model, who shall act in the management and compliance with the guidelines.

☒ The CONTRACTED PARTY must clearly and objectively have an Information Security Policy or similar document, which contains security guidelines. This must be periodically reviewed and disclosed to all employees and third parties.

☒ The CONTRACTED PARTY's Information Security Policy should address, but not be limited to, the following items:

a) Information Classification;
b) Clean Table and Screen;
c) Physical Security;
d) Access control;
e) Passwords;
f) Information Handling;
g) Software License;
h) Backups;
i) Incident Response;
j) Internet Access;
k) Use of Electronic Mail;
l) Documented Procedures;
m) Vulnerability/Patches Management.

☒ The CONTRACTED PARTY shall document and keep updated the internal processes and procedures related to the provision of the service and the information security requirements (ISO 27002:2013).

☒ The CONTRACTED PARTY must carry out, during contracting and periodically, awareness training for its employees on the aspects of Information Security required in this document.

☒ The CONTRACTED PARTY must comply with the legislation and regulations applicable to the provision of services, particularly the General Telecommunications Law (9,472/1997).

☒ The CONTRACTED PARTY must comply with the General Data Protection Law (13,709/18).

☒ The CONTRACTED PARTY must designate responsible people, custodians and users of the information in its internal systems.

☒ If the service provided involves payment card transactions, the CONTRACTED PARTY must comply with the PCI-DSS standard.

a) Annually, the CONTRACTED PARTY shall demonstrate compliance in accordance with the PCI rules, banners and purchasers;
b) All information owned by CLARO, as well as information from its customers and employees, must have its use restricted to the provision of the contracted service and must be treated as confidential.

2.1 SECURITY INCIDENTS

☒ The CONTRACTED PARTY must immediately notify CLARO of the occurrence of incidents, irregularities or suspicious events that affect or may affect the security of CLARO's proprietary information, under the terms of

[Signature]

GERÊNCIA CONTRATOS CLARO JURÍDICO PAL

the Agreement.

☒ The CONTRACTED PARTY shall ensure that the logs for analysis or expertise are available when requested by CLARO.

2.2 SAFE DEVELOPMENT

☒ The CONTRACTED PARTY must guarantee the basic assumptions of information security (confidentiality, integrity and availability) for all systems and/or applications proper to fulfill the Agreement object that handle CLARO data or information.

☒ The CONTRACTED PARTY must comply with all guidelines and controls described in Annex A ("Safe Development Guidelines").

3 ACCESS MANAGEMENT

3.1 AUTHENTICATION

☒ The CONTRACTED PARTY's employees must use an access credential in order to be able to recognize (identification) and prove (authentication) the user's identity when accessing the information systems, resources, data processing areas and communications networks that support the operation of the CONTRACTED PARTY.

☒ Each employee who needs access to comply with the Agreement object will have its own access credential, and sharing or use of generic users is not allowed. Likewise, every access credential will have an owner who will be responsible for the actions that are taken.

☒ Passwords must be personal and non-transferable.

☒ All access credentials that have not been used for a maximum period (configurable) must be disabled. This period must be included in the CONTRACTED PARTY's policy or procedures.

☒ All credentials of users who have been dismissed or whose services have been discontinued must be disabled and maintained for a period (configurable), to avoid loss of history or logs.

☒ Upon dismissal of a CONTRACTED PARTY's employee involved in the operation of the service provided to CLARO, the CONTRACTED PARTY must immediately provide for the cancellation of all access.

3.2 AUTHORIZATION

☒ Any user who needs to obtain an access credential on any system must go through an authorization process. The process must contemplate and formalize all steps of REQUEST, APPROVAL, EXECUTION, DELIVERY AND PASSWORD EXCHANGE.

☒ All requests to release access to information, systems and/or resources must be formally approved by CLARO.

☒ User profiles must be defined according to the need for use and also aligned with business requirements.

☒ A secure password delivery process must be set.

☒ The systems and/or applications used in the provision of the contracted service must provide for their use by users with access credentials who have the minimum privilege necessary to exercise their function, and there should be no need to increase the privileges of these users to perform them.

4 AUDIT LOGGING

☒ The CONTRACTED PARTY must generate and provide to CLARO, records that identify all the actions performed by the CONTRACTED PARTY's employees so that it is possible to identify the operator who performed each action performed, the time of execution (date/time) and from what equipment it was performed.

☒ The log files must be stored securely and have restricted access, especially in cases of permission to change and delete. Access and reading of the log files must be restricted to authorized users.

☒ There should be no process or function that changes or deletes any record in the audit trail, except the retention script.

☒ System administrators should not be allowed to delete or disable logging.

☒ The environment clock synchronization must be carried out in order to ensure the accuracy of the times of

[Signature]

GERENCIA CONTRATOS CLARO JURÍDICO PAL

occurrence and credibility of the events recorded in the logs.

☒ Confidential data used to authenticate access credentials (passwords, private keys etc.) or to authorize access (session IDs or passwords etc.) must not be recorded in the log files.

☒ The CONTRACTED PARTY's assets that support the Agreement object must provide at least, but not limited to:

a) User login;
b) Date;
c) Time;
d) Event type;
e) IP address and host name of the equipment.

4.1 STORAGE PERIOD

☒ The log files of systems, resources and networks that process information object of the Agreement must be stored online for a minimum period of six (6) months and one (1) year offline.

☒ The CONTRACTED PARTY must define a process and a person responsible for making the log files available to CLARO.

☒ CLARO may request access to the system log files at any time.

5 DATA PROTECTION

☒ All information and personal data and sensitive personal data of CLARO customers and employees must be encrypted during processing, storage and transmission.

☒ The encryption process must meet the following conditions:

- There must be key management, including methods for dealing with the protection of cryptographic keys and the recovery of encrypted information, in the case of lost, compromised or damaged keys;
- The use of FIPS 140-2 compliant cryptography modules or equivalent secure standard for the management and use of cryptographic keys must be preferred;
- There should be procedures that include requirements for the management of cryptographic keys throughout their entire life cycle including, generation, storage, archiving, recovery, distribution, removal and destruction of the keys;
- All cryptographic keys must be protected from modification and loss. In addition, secret and private keys need protection against unauthorized use or disclosure;
- Use of equipment to generate, store and save keys must be physically protected;
- In the authentication process using public key certificates, they must be issued by a certifying authority, which is a recognized organization, with adequate controls and procedures in place to ensure the required level of trust.

☒ According to CLARO's safety rules and policies, the following must be met for their transmission:

a) Be encrypted to maintain the confidentiality, integrity and traceability of information;
b) Be controlled, in accordance with the relevant legislation;
c) Be protected against interception, copying, modification, diversion and destruction;
d) Use a secure protocol and solutions for communication between the parties with guaranteed end-to-end communication.

5.1 DISPOSALS

☒ The information obtained through the Agreement object, stored, processed and transmitted, must be destroyed using techniques and tools that prevent recovery after termination of the Agremeent, when requested by CLARO.

6 VULNERABILITY MANAGEMENT

☒ The CONTRACTED PARTY shall maintain an updated database or inventory tool on technological assets, operating systems and base software installed at the company, which includes information on manufacturers, versions, patch update levels and, in the case of base software, the operating system in which it is installed.

☒ The CONTRACTED PARTY must implement security patches, as made available by the respective manufacturers of the software that supports the operations.

☒ The CONTRACTED PARTY must deliver to CLARO every three (3) months a report with a treatment plan for the identified vulnerabilities. The result of the work cannot contain critical vulnerabilities.

☒ The CONTRACTED PARTY must define a procedure to calculate the risk of each identified vulnerability,

[Signature]

GERENCIA CONTRATOS CLARO JURÍDICO PAL

considering criteria for classification of information, probability of exploitation of the vulnerability and the related impact.

7 BUSINESS CONTINUITY MANAGEMENT

☒ Availability of environments, as contracted, considering the type of activity to be performed:

a) a) The CONTRACTED PARTY shall provide at any time, when requested by CLARO, the information regarding the infrastructure that supports the activities, as well as the mapping of the locations and the name of work/operation stations available in each of the locations where they are provided;
b) b) CLARO must provide an assessment of eligible businesses and priority for recovery of activities.

☒ The CONTRACTED PARTY shall inform CLARO of any and all changes in infrastructure and/or resources in its work environment and in the contingency environments that act or make any reference to the object now contracted for the perfect fulfillment of this clause.

☒ The CONTRACTED PARTY shall implement the Business Continuity Management System: Crisis Management Plan (example: water and electric crisis), Incident Management Plan, Disaster Recovery Plan, Operational Contingency Plan, Test and Validation Plan and Communication Plan.

☒ The maximum and minimum term/time for recovery of data and/or services in case of disasters must be defined and documented between the CLARO Agreement Manager and the CONTRACTED PARTY.

☒ Tests of contingency plans and elements should be carried out periodically, with evidence collections.

☒ The CONTRACTED PARTY must guarantee the backups of information and periodically perform restoration tests.

☒ The CONTRACTED PARTY must have contingency infrastructure: generators, no break, redundancy of web page hosting servers, link redundancy, redundancy of critical equipment for operation, cooling, water reservoirs, alternative site etc.

☒ The CONTRACTED PARTY's resources involved in the Business Continuity Plans (BCP), must be trained in the theme, according to their attributions and responsibilities in the plans.

☒ Tactical solutions to support the restoration of the required activities within a desired recovery time must be identified. In each case, alternatives must be evaluated in order to minimize the likelihood that the same incident will affect the business continuity solution.

☒ Any and all incidents that compromise the Continuity of Services, must be immediately communicated to the responsible Agreement Manager, for the necessary measures and, if needed, to activate the respective Continuity Plans.

☒ Procedures for responding and stabilizing the situation after an incident must be developed and implemented, using specific response plans for each type of scenario assessed after the risk analysis has been carried out.

8 ENVIRONMENT LOGICAL SAFETY

The operations installed in the CONTRACTED PARTY's environments/sites must:

☒ Provide an exclusive and segregated network segment for the services contracted by CLARO.

☒ Control and restrict access from other networks to the exclusive network used to provide the service, through restrictive firewall rules.

☒ Provide, when requested by CLARO, updated physical and logical diagrams of the networks that support the operations covered by the Agreement, containing the equipment used and their interconnections.

☒ Provide continuous security monitoring of network traffic.

☒ Implement Internet communication control rules according to the operation's need.

☒ Create access profiles for internal systems related to operations, obeying the principles of minimum privilege and segregation of functions.

☒ Protect the company's network connections from other external networks, in accordance with Information Security best practices (ISO 27002 and NIST.

☒ The CONTRACTED PARTY's assets must provide protection against malicious codes, such as anti virus and personal firewall (keep them updated daily).

[Signature]

GERENCIA CONTRATOS CLARO JURÍDICO PAL

☒ The installation and use of wireless access points (IEEE 802.11 standard) must be controlled. The administration interface for network equipment, computers and wireless access points should be accessed only by authorized users.

☒ Wireless access points must be configured according to secure communication standards (e.g.: WPA2 or higher).

☒ The assets involved in providing the service to CLARO must be covered by a hardening process, as follows:

- o Shall establish, document, publish and make available the Operational Security Procedures (Hardening) for each type of information technology asset that processes, stores or transmits information owned by CLARO, such as servers, workstations, operating systems, databases, network equipment, application servers etc;
- o Must ensure that these procedures cover all known security vulnerabilities. As a source of information, vulnerabilities and controls, one can include external and trusted sources, such as the Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin Audit Network Security Institute (SANS) and National Institute of Standards and Technology (NIST).

- In addition to the guidelines in this document, the operational security procedures must include at least the following controls:

  - Default passwords and parameters, such as root, administrator and guest passwords, registry keys, community names, host names and others must be changed before the asset is made available for production;
  - The default credentials for administrative, privileged, root and similar access must be kept securely, preferably under double control and divided knowledge, for as few employees as possible;
  - Unauthenticated, anonymous or guest access must be disabled;
  - Inactive accounts must be removed or blocked periodically;
  - Actives must have only one main function;
  - All administrative or support access performed by the network, or which is not performed by the physical console of the active, must be encrypted;
  - Unapproved IM ("Instant Messaging") applications must be removed;
  - Peer-to-peer data sharing (P2P) programs must be removed;
  - Any privileged password provided to technicians or auditors for maintenance or audit actions must be changed immediately after the maintenance or audit is completed;
  - The active must have only connections and interfaces (dial-up, Ethernet, WiFi, optical fiber and others) necessary for its purpose;
  - Entertainment programs (games and the like) must be removed;
  - Secondary operating systems must be removed from the asset;
  - Installation and configuration procedures must be documented;
  - The hardware of the actives must be updated according to the processing, storage and communication needs;
  - Assets must be configured to not boot from removable media;
  - Services, subsystems and other components that are not strictly necessary for the asset to function must be removed or disabled;
  - Demo packages, examples and the like must be removed from assets in a production environment;
  - File system permissions must be configured as restrictively as possible;
  - Access to administration commands and tools should be restricted to administration and support personnel;
  - Configuration parameters (configuration files, registry keys and the like) must be configured in accordance with the best security practices;
  - Changing configuration parameters must be restricted to asset managers;
  - The startup or operation of the asset in debug mode must be controlled and restricted to situations where this need is justified and must be activated only by the administrators;
  - The contents of the RAM memory must be protected against discharges (or dumps) in case of failures or exceptions;
  - The asset must have protections against unauthorized changes to the name-resolution system (DNS);
  - The asset must have a time synchronization mechanism with internal time servers and these must receive the time from trusted external sources;
  - Routing between networks must be disabled on equipment that has not been installed for this specific function;
  - Services and applications must be executed in a restrictive user context, with only the privileges strictly necessary;
  - Assets installed in a production environment must not have test, development or certified data or accounts;
  - Licensing schemes for operating systems, applications and other systems must be respected;
  - The list of commands, programs and actions performed automatically when the asset is started should be checked periodically for malicious commands;
  - Unnecessary network interfaces and protocols must be removed;
  - There must be a method for backing up CLARO's information and it must be tested periodically;
  - Only the protocols and websites necessary for the execution of the contracted services should be released for user accesses;
  - Disable unnecessary services and functionality on computers and network equipment that support CLARO's operations;
  - Servers must be stored in secure locations;

[Signature]

GERENCIA CONTRATOS CLARO JURIDICO PAL

- The CONTRACTED PARTY shall restrict physical access to publicly accessible network points, wireless points, gateways and portable devices;
- Computers must be locked after fifteen (15) minutes of inactivity and must only be unlocked using the user password;
- The equipment involved in the operation must have only connections, interfaces, applications and devices necessary for its purpose. The CONTRACTED PARTY must block the use of devices that allow the recording of information on media, such as:
  - ✓ CD-RW;
  - ✓ DVD-RW;
  - ✓ Hand held computers;
  - ✓ Digital cameras and any other type of equipment that contains photography resources;
  - ✓ Cell phones with cameras;
  - ✓ iPods;
  - ✓ Tablets;
  - ✓ Recorders;
  - ✓ Camcorders;
  - ✓ Pendrives;
  - ✓ Any other media or peripherals that allow the recording of CLARO information.
- The CONTRACTED PARTY must present the logical security requirements currently implemented in its operation, as well as improvement projects already underway;
- The audio recording system used to provide the service to CLARO must be in a controlled environment with restricted access.

9 SECURITY TESTS

☒ The CONTRACTED PARTY shall allow CLARO to carry out the necessary safety tests when requested on systems, sites, applications etc. object of the Agreement.

☒ The result of the test will be sent to the CONTRACTED PARTY who must return an action plan within thirty (30) days stating the deadlines for correcting the identified vulnerabilities.

10 10 COMPLIANCE DILIGENCES

☒ The CONTRACTED PARTY undertakes to maintain, throughout the performance of the Agreement, in compliance with the obligations assumed by it, all the conditions required below:

- The CONTRACTED PARTY shall respond to reports and send evidence requested by the Information Security and Business Continuity Division, containing a self-assessment of the security requirements determined in the Agreement;
- Physical and logical environments for receiving, processing and manipulating data/information covered by the Agreement may undergo periodic security inspections designated by the Information Security and Business Continuity Division;
- The CONTRACTED PARTY must allow CLARO employees, at any time, to proceed with the CONTRACTED PARTY's verification of compliance with the controls included in the Agreement, as well as allow the analysis and verification of its attendance and service enabling procedures;
- The identified non-conformances must be corrected and an Action Plan must be sent to the CONTRACTED PARTY with a deadline for regularization. Vulnerabilities classified as HIGH, according to the CONTRACTED PARTY's own risk analysis methodology, cannot be corrected within a period of more than thirty (30) days.

11 11 TERMINATION OF THE AGREEMENT

☒ The replacement or even the termination of the services provided can occur at any time, for that some security items must be followed:

- Review of the Agreement and confidentiality clauses;
- Guarantee of revocation of accesses;
- Destruction of stored data;
- Delivery of all telephone recordings and stored logs;
- Review of business continuity plans involving the CONTRACTED PARTY;
- The deadline for making the due adjustments must be provided for in the Agreement;
- Care must be taken to verify that the clauses of the Agreement are being met, especially those related to the destruction of information and revocation of accesses.

12 FINAL PROVISIONS

☒ The CONTRACTED PARTY must preserve CLARO's information and assets, using them strictly for the performance of its functions and complying with the policies, safety rules and procedures defined for the operation of the contracted object.

☒ The CONTRACTED PARTY is responsible for any fraud originating from the failure to comply with the defined procedures, regardless of the existence of systemic locks.

[Signature]

GERÊNCIA CONTRATOS CLARO JURÍDICO PAL

- ☒ The resources made available by CLARO, including systems, applications and apps, must be used for purposes related to the contracted object, and any use of the resources for illegal and/or profitable purposes as well as commercial or professional purposes other than those permitted by the company is prohibited.

- ☒ The CONTRACTED PARTY must notify as soon as possible about the occurrence of suspicious incidents or events that affect or may affect the security of information and the business, through the procedures and channels defined by CLARO.

- ☒ It is prohibited to take advantage of the vulnerabilities or weaknesses that may exist in the systems.

- ☒ The model of access through home office of the information and data of CLARO customers and employees is not allowed.

- ☒ The CONTRACTED PARTY must have a technological solution that integrates/authenticates the attendant in our systems/applications.

- ☒ The CONTRACTED PARTY must not use any type of robotization solution or even unique Front-End to access our systems/applications.

[Signature]

GERENCIA CONTRATOS CLARO JURÍDICO PAL

ANNEX A - SAFE DEVELOPMENT GUIDELINES

To guarantee the basic assumptions of information security (confidentiality, integrity and availability), appropriate security controls should be used in systems, applications and/or apps that manipulate or store information owned by CLARO.

1 Security Architecture

The purpose of the security architecture is to define some security assumptions related to the network infrastructure and important operational details to ensure the security of the system:

a) The developed systems must follow the three-layer model - Presentation, Application and Database Layer, logically segmented, with at least the Presentation Layer physically separated from the Database Layer, that is, each one on a server;
b) For applications aimed at the public, accessible through external networks, these must be segregated from the internal network to avoid compromising the environment, so these applications must be implemented in the DMZ;
c) Systems that need to access the Internet to search for updates must be released in the application proxy and restricted to specific URLs;
d) The project must include an updated logical design detailing: the components of the solution and a brief description of them; the communication flow between the components of the solution with a brief description;
e) Releases of communication ports must be approved by Information Security before being configured;
f) Internal systems must be restricted to the internal network;
g) The system must be compatible with the security rules defined for the infrastructure of the servers that will host the system;
h) Off-the-shelf software must follow the requirements for secure development. They must have as little privilege as possible to perform their functions. Operating system administrator access must be restricted;
i) All humanized channels, that is, those that have interaction with the user, must have HTTPS certificate. For external channels, these certificates must be recognized by an external CA, for internal users it is acceptable to use an internal CA;
j) Sensitive information must travel through an encrypted connection and in a secure manner;
k) Unnecessary services such as scripts, drivers, resources, subsystems and unnecessary file systems must be removed on development, approval and production servers;
l) Plug-ins or tools not approved in the environment should not be installed, if necessary, it must be aligned with Information Security;
m) Outdated or unsupported components should not be used to compose the application;
n) It is mandatory to have a functional certified environment, before the system is ported to the production environment;
o) The developed system must identify high availability requirements;
p) Administrative interfaces, those used to maintain the application, must be restricted to the internal network;
q) The project must point out the information that needs to be considered in the existing backup process;
r) All projects must include a contingency plan for the system;
s) All systems, applications and/or apps development projects must include tests and controls to prevent the main threats (TOP 10 OWASP):
   A1 - Injection;
   A2 - Breach of Authentication and Session Management;
   A3 - Exposure of Sensitive Data;
   A4 - External XML Entities (XXE);
   A5 - Breach of Access Control;
   A6 - Incorrect Security Settings;
   A7 - Cross-Site Scripting (XSS);
   A8 - Unsafe deserialization;
   A9 - Use of Vulnerable Components;
   A10 - Insufficient Registration and Monitoring.

2 General Coding Practices

The objective is to ensure that confidential data is accessible only to authorized users:

a) Use APIs that embed specific tasks to perform operating system tasks. Do not allow the application to execute commands directly on the operating system, especially through the use of command shells initiated by the application;
b) Use checksum or hash integrity verification mechanism to verify the integrity of interpreted code, libraries, executable files and configuration files;
c) Protect shared variables and resources from inappropriate competing accesses;
d) Passwords or keys should not be stored in the source code;
e) Applications must be developed to run with minimal privilege;
f) Do not directly transfer data provided by the user to any function, with dynamic execution, without first performing the data processing in an appropriate manner (see section CRITERIA FOR THE CREATION OF ACCESS PROFILES);
g) Review all secondary applications, codes and third-party libraries to determine the business need and validate security features, as these may introduce new vulnerabilities;
h) Implement updates in a secure way. If the system should perform automatic updates, then it must use digital

[Signature]

GERENCIA CONTRATOS CLARO JURIDICO PAL

signature mechanisms to ensure the integrity of the code and ensure that customers and employees verify the signature after downloading. Use encrypted channels to transfer the code from the server host;

i) Disable the functionality to remember the password (auto-complete) in the password fields of the browser.

3 User Account Credentials

All access credentials for internal systems must be in accordance with the document prepared precisely for that purpose (Standard for Logical Access to Computerized Resources).

For external systems, this TECHNICAL GUIDELINE FOR SAFE DEVELOPMENT should be used.

3.1 Authentication

a) The information related to an access credential must be kept, even after deactivation, so that its history or logs are not lost;
b) The systems must provide for the creation of user profiles integrated with the authentication systems approved and in use by CLARO, with their access control centralized by the area responsible for Access Control;
c) The system credentials must be stored in a database with the encrypted information;
d) Users must be re-authenticated before performing critical operations. Use multi-factor authentication for highly sensitive accounts or applications with high financial value;
e) All systems, applications and/or apps that require maintenance and are exposed on the Internet must use two authentication factors (e.g: Mobile Token);
f) Validate authentication data only at the end of all data entries, especially for sequential authentication implementations;
g) Responses for authentication failures should not indicate which part of the authentication data is incorrect. For example: instead of displaying messages like "Incorrect username" or "Incorrect password", just use messages like: "Invalid username and/or password", for both error cases. Error responses must be literally identical in both cases;
h) Password reset processes and change operations must require the same levels of control as for account creation and authentication;
i) Require changing temporary passwords the next time the user authenticates to the system;
j) If you are going to use third party code to authenticate, it is necessary for Information Security to inspect code to ensure that it is not affected by any malicious code.

3.2 Authorization

a) The system projects must provide for their use by users with access credentials who have the minimum privilege necessary to exercise their function, and there should be no need to increase the privileges of these users to perform them;
b) The application user used to authenticate with the database must be identified by the project, must have restrictions on the use of the network and must be blocked for any other access;
c) All systems access to databases must be done through an intermediate layer, using resources such as store procedures, views, COM+ components, Web Services, Enterprise Services, Remote, NET and/or other resources that guarantee access security.

4 Criteria for Creating Access Profiles

a) Nomenclature of the functional profile:

☒ The profile name should reflect the business function associated with it, making the purpose of the profile clear to anyone who sees the name. Example: TV PACKAGE INCLUSION, INTERNET PACKAGE INCLUSION, ADDRESS CHANGE.

b) Access authorization structure:

☒ The systems must, in their access authorization structure, meet the function levels, functional profiles and functionalities, according to the example:

LOCATION	FUNCTION	FUNCTIONAL PROFILE	SYSTEMIC FUNCTIONALITY
CALLCENTER	MASSIVE SERVICE	CHANGE ADDRESS	AI REGISTRATION CONSULTATION SCREEN

c) Function:

☒ Each function must be composed only and by the functional profiles relevant to the fulfillment of its activities. System users have their privileges granted when linked to a function.

d) Functional profile:

☒ Each functional profile must be composed of the systemic functionalities relevant to the defined business

[Signature]

GERÊNCIA CONTRATOS CLARO JURÍDICO PAL

function. Every profile must be created considering the concept of "minimum privilege", that is, it must have the least amount of access possible to the systemic functionalities necessary to perform a business activity (function).

e) Systemic functionalities:

☒ All systemic functionalities must be associated with some functional profile. The same functionality can be associated with several profiles.

5 Error Handling and Audit Trails (Logs)

a) Do not expose sensitive information in error responses, including system details, technologies, session identifiers or user account information;
b) Use error-handling mechanisms that do not display debug information or exception stack information;
c) CLARO standard error messages should be displayed to the customer. Use the reroute code (3XX), which indicates that something more needs to be done or needed to be done to complete the request;
d) The handling of logical errors associated with security controls should deny access by default;
e) All log controls must be implemented in a system separate from the application;
f) In addition, all systems must include audit trails;
g) Access and reading of the log files must be restricted to authorized users;
h) Confidential data used to authenticate access credentials (passwords, private keys etc.) or to authorize access (session IDs or passwords etc.) must not be recorded in the log files;
i) The system, application and/or app must record at least the following events, when applicable: access to sensitive data, administrative user actions, access to audit trails, invalid access attempts, use of authentication and identification mechanisms, audit log initialization, input data validation failures, connection attempts with invalid or expired session tokens, TLS connection failures with the backend and encryption failures;
j) The system should provide at least the following records for each log entry: user identification, type of event, date and time, indication of success or failure, origin of the event and data identification, component, resource or related object;
k) Use a cryptographic hash function to validate the integrity of the log records.

6 Validation of Entries

a) All data entry points must be identified in the project;
b) All parameters and input data, including form fields, hidden fields, query strings, cookies and HTTP headers, must be validated by at least:
   ☒ Type;
   ☒ Lenght;
   ☒ Existence of invalid characters;
   ☒ Format;
   ☒ Range.
c) Validate expected data types, data range, data length and whenever possible validate all input data using a white list method that uses a character or regular expression list that defines the characters allowed;
d) All data sent by users must be validated on the server;
e) The input data validation routine must be centralized in the system;
f) Security decisions must be made on the server and must not depend on profile data or permissions provided directly by the client (in web applications, including variables in cookies, hidden form fields, GET or POST parameters and the like);
g) Controls must be implemented to inhibit the entry of data or scripts in the URL;
h) Specify appropriate character sets, such as UTF-8, for all data input sources;
i) Encode the data to a common character set before validation (Canonicalize);
j) Perform context-based treatment (sanitization) of all data from untrusted sources used to build SQL, XML and LDAP queries;
k) If any potentially "dangerous" characters need to be allowed in the system's data entry, make sure that additional controls such as encoding the output data, specific APIs that provide secure tasks and audit trails in the use of the data by the system have been implemented. As an example of "potentially dangerous" characters, we have the following: <, >, ", ', %, (,), &, +, \, \', \";
l) If the standard validation routine does not address the following entries, then they should be checked discreetly:
   ☒ Check for null bytes (% 00);
   ☒ Check for newline characters (%0d, %0a, \r, \n);

☒ Check for dot-dot slash characters (../ or ..\) that change paths. In the case of character sets that use UTF-8 extension, the system should use alternative representations such as: %c0%ae%c0%ae/. Canonicalization should be used to solve problems of double encoding (double encoding3) or other forms of attack obfuscation.

7 System configuration

a) The application must not be installed using standard parameters such as: paths and directory names, passwords, user name or key, dataset, among others;
b) Communication channels for remote administration must be protected;
c) Use only POST requests to transmit authentication credentials. Do not expose session identifiers to URLs, error messages or logs. Session identifiers should only be found in the HTTP cookie header. For example, do not

[Signature]

GERENCIA CONTRATOS CLARO JURÍDICO PAL

traffic session identifiers in the form of GET parameters;
d) Use mechanisms complementary to the standard session management mechanism for sensitive server-side operations, such as account management operations, through the use of random tokens or parameters associated with the session. This method can be used to prevent Cross Site Request Forgery attacks;
e) Use complementary mechanisms to the session management for highly sensitive or critical operations using random tokens or parameters in each request;
f) Configure the "secure" attribute for cookies transmitted over a TLS connection;
g) Configure cookies with the HttpOnly attribute, unless it is explicitly necessary to read or set the values of the cookies through scripts on the system client side;
h) Use the "referrer" field in the header only as a form of supplementary verification. It should not be used alone as a form of authorization check, as the value of this field can be tampered with;
i) Do not provide Servlets that control through parameters, access credentials and navigation rules;
j) Disable the auto-complete functionality on forms that contain sensitive information, including the authentication form;
k) Disable caching on the client side of pages that contain sensitive information. The Cache-Control: no-store parameter can be used in conjunction with the control defined in the HTTP headers "Pragma: no-cache", which is less effective, but compatible with HTTP/1.0;
l) Disable directory listing;
m) Prevent the disclosure of the directory structure by preventing search robots from indexing sensitive files, through the correct configuration of the robots.txt file, defining directories that must be inaccessible to these indexers in an isolated underlying directory. Thus, access to the parent directory defined in the robots.txt file must be disabled instead of disabling each directory individually;
n) Disable unnecessary HTTP methods, such as WebDAV extensions. If it is necessary to use an extended HTTP method to support file manipulation, then use some well-controlled authentication mechanism;
o) Remove unnecessary information present in HTTP response headers that may be related to the operating system, web server version and application frameworks;
p) Implement WS-Security which is a SOAP extension to enforce security for web services.

8 Encryption

a) All data and information must be treated in accordance with the official CLARO Information Classification criteria;
b) The use of cryptographic keys must be controlled by market tools and formalized;
c) The use of the key as an application and purpose must be documented;
d) Cryptographic keys must be provided only to authorized personnel, and with formal authorization from the information owner;
e) The cryptographic keys used must be stored in a secure location, so that only personnel authorized by the responsible area have access;
f) The use of FIPS 140-2 compliant cryptography modules or equivalent standard for the management and use of cryptographic keys must be preferred;
g) Keys used to encrypt other keys, also known as key encryption keys, must be at least as robust as the keys protected by them;
h) The system must have mechanisms to prevent unauthorized substitution of cryptographic keys;
i) All software, functions and cryptographic libraries used in the systems must have been previously certified and approved by the responsible areas at CLARO;
j) All cryptographic keys must be changed periodically through a key change ceremony.

9 Session Management

a) Encrypted protocols, such as HTTPS/TLS, should be used to protect sensitive data transmitted over the network;
b) Use server-based or framework-based session management controls. The system should recognize only the session identifiers as valid;
c) The creation of session identifiers must always be performed in a reliable system, for example: centralize all control on the server;
d) Use appropriate algorithms that guarantee the randomness of the session identifiers;
e) The logout functionality must completely end the session or associated connection;
f) The session must be limited to a maximum of 15 (fifteen) minutes of inactivity;
g) If a session was established before login, then this session must be closed for establishing a new session after login;
h) Generate a new session identifier when there is any new authentication;
i) Do not allow simultaneous connections with the same user identifier;
j) Generate a new session identifier and periodically disable the old identifier. This can mitigate certain scenarios of session hijacking attacks, when the original session identifier is compromised;
k) The session state must be protected from unauthorized access.

10 Access Control - Systematic Controls

a) Use only system objects that are trusted, as with server session objects, to make access authorization decisions;
b) Use a single component throughout the system to perform the access authorization verification process. This includes libraries that invoke external authorization services;
c) Deny all access if the system is unable to access the information contained in the security configuration;
d) Ensure authorization controls on all requests, including server-side scripts, "includes" and requests from client.

[Signature]

GERENCIA DE CONTRATOS CLARO JURÍDICO PAL

side technologies;
e) Restrict access to protected functions, direct reference to objects, services and system data to authorized users only;
f) Restrict access to user attributes and data, as well as information on regulations used by access control mechanisms;
g) Restrict access to relevant security settings to authorized users only;
h) Limit the number of transactions that a single non-robotic user, through CAPTCHA or some control that determines a time to the access attempts;
i) If authenticated and active sessions are allowed to remain for long periods of time, periodically revalidate the user's authorization to ensure that their privileges have not been modified and if they are, perform user logging and require new authentication.

11 Data Protection

a) Confidential data, personal data, sensitive personal data of employees/third parties stored in a database must be encrypted;
b) A transactional control mechanism in the database (Commit/Rollback) must be contemplated;
c) The routing of connections to the database must always be from the application layer, there should never be any user computer, developer or support directly connected to the database on production systems;
d) The development and certification process of the systems must be carried out only with masked databases and/or fictitious data, however the same structure of the original production bases and sufficient data volume for the execution of the tests must be maintained, aiming at carrying out simulations compatible to the business reality;
e) Do not store passwords, connection strings or other confidential information in clear text or in any way unsafe on the client side;
f) Remove unnecessary applications and system documentation that may disclose important information to malicious agents;
g) The system should support the removal of confidential data, personal data and sensitive personal data when they are no longer needed.

12 Communications Security

a) Use encryption in the transmission of all sensitive information. This must include TLS (latest secure and stable version) to protect the connection and must be supplemented by encrypting files that contain sensitive data or connections that do not use the HTTPS protocol;
b) TLS certificates must be valid, have the correct domain name, have not expired and be installed with intermediate certificates, when necessary;
c) When TLS connections fail, the system must not return an insecure connection;
d) Use a single TLS implementation standard that is properly configured;
e) Specify the character encoding for all connections.

13 System Compliance

a) Ensure that servers, frameworks and system components are running the latest approved version;
b) Ensure that servers, frameworks and system components have the latest patches applied to the version in use;
c) Remove all unnecessary features and files;
d) Remove the test code or any unnecessary functionality for the production environment, before the system is implemented;
e) The storage of the security configuration for the system must be capable of being produced legibly to support the audit;
f) Implement a change control system to manage and record changes to the code, both in development and in production systems. Change control must include at least impact documentation, documented approval of change by authorized parties, functionality testing to verify that the change has no adverse impact on system security, and reversal procedures.

14 Database Security

a) Use strongly typed queries and parameterized variables, that is, once the query has been parameterized, it should not be changed;
b) Use input validation and output encoding and ensure the meta character approach. If it fails, the command in the database must not be executed;
c) Perform meta characters escaping in SQL statements;
d) The system must use the lowest possible level of privileges when accessing the database;
e) Use individual credentials to access the database. Do not use generic or administration accounts to access, for example, admin, root or sys;
f) Connection strings must not be coded in the application. The connection string must be stored in a separate configuration file on a trusted system and the information must be encrypted;
g) Use stored procedures to abstract access to data and allow removal of permissions from tables in the database;
h) Remove or modify all default passwords for administrative accounts. Use strong passwords (unusual or difficult to deduce) or implement multi-factor authentication. Disable any unnecessary functionality in the database, such as unnecessary stored procedures or services. Install the minimum set of components or options required (method of reducing the surface area);
i) Eliminate unnecessary content included by default by the supplier, e.g.: example schemes;

[Signature]

GERENCIA CONTRATOS CLARO JURIDICO PAL

j) Disable all accounts created by default and that are not required to support business requirements;
k) The system must connect to the database with different security credentials for each type of need, such as: user, read-only, guest, administrator etc.

15 File Management

a) Request authentication before allowing a file to be uploaded and downloaded;
b) Limit the types of files that can be uploaded to accept only the types that are necessary for business purposes. Restrict file upload of extensions of type: CMD, BAT, SCR, EXE, VBS and WS;
c) Validate that the files sent are of the expected type by checking the headers. Performing a file type check by extension alone is not enough;
d) Disable execution privileges on file upload directories;
e) When referencing existing files, use a white list of allowed file names and types. Perform the validation of the passed parameter value and if it does not correspond to what is expected, reject the entry or use a file value specified by default by the application;
f) Do not pass parameters of paths of directories or files in requests. Use some mechanism for mapping disk paths to indexes that are passed on to users and serve to be mapped in a pre-defined list of file paths;
g) Make sure that system files and resources are read-only;
h) Scan files that users have submitted via upload mechanism in search of digital threats (Viruses, Ransomware, Rootkits, among others).

16 Memory Management

a) Check if the buffer is as big as the one specified;
b) When using functions that accept a certain number of bytes to make copies, such as strncpy(), be aware that if the size of the destination buffer is equal to the size of the source buffer, it cannot contain the null string;
c) Check the buffer limits if the function calls are made in a loop and verify that there is no danger of writing beyond the allocated space;
d) Truncate all input strings to a reasonable length before passing them on to the copy and concatenation functions;
e) End resources specifically, not counting the garbage collector in releasing resources allocated for connection objects, file identifiers etc.;
f) Use non-executable batteries, when available;
g) Avoid using functions known to be vulnerable, for example: printf, strcat, strcpy etc .;
h) Free the appropriately allocated memory after completing the subroutine (function/method) and at all output points.

SYSTEMS FOR MOBILE DEVICES

a) Any system developed for mobile platforms, such as Android, IOS or others, must comply with the requirements below. This is necessary to avoid exploiting common vulnerabilities in applications on these platforms, which have unique characteristics in relation to desktop systems and web applications;
b) The requirements below are complementary to those mentioned above and must be applied according to the application platform.

1 System configuration

a) Unique device ID values should not be used as a security control;
b) The application must be signed with a valid digital certificate;
c) The application must not store secret keys or passwords in its executable code;
d) The application for internal use, that is, for employees, must disable features of print screen or auto-snapshot, to prevent sensitive information from being disclosed by this functionality;
e) The application must not be run on a device with changes to its operating system. Traditionally these techniques are known as "Root Device" in the case of Android systems and "Jailbreaking" in the case of iOS systems;
f) The permissions and files requested by the application for its correct functioning must follow the principle of least privilege;
g) The application's binary files must be obfuscated to avoid attacks that use reverse code engineering techniques;
h) All test data must be removed from the application's container (.apk, .ipa and .bar files, among others);
i) The application must validate its configuration files to assess whether they have been changed to insert unsafe variables, such as debug flags, read permissions etc.;
j) The application must use the minimum permissions necessary for its operation. This contributed to guarantee the privacy of users and the system usability;
k) The application must not create files with global permissions on the device's file system, such as MODE_WORLD_READABLE or MODE_WORLD_WRITABLE. The principle of least privilege should be used to prevent excessive permissions granted to an application from compromising the security of the mobile device;
l) The application must keep the access credentials (user and password) in memory for as little time as possible, just enough to complete the validation process;
m) The application must discard and clear all memory associated with user data and all master keys used to decrypt sensitive data;
n) Support for JavaScript and Plugins must be disabled for any WebViews;
o) The file access system must be disabled for any WebViews, such as "webview.getSettings ()" and "setAllowFileAccess (false)", preventing web applications from accessing the application's local content;
p) All services must completely filter and validate the entries from the application. When handling with dynamic

[Signature]

GERENCIA CONTRATOS CLARO JURIDICO PAL

queries or "ContentProviders" it must be ensured that parameterized queries are being used;

q) You should restrict the use of application debugging mode by avoiding easy manipulation at run time by an attacker or malware. This is usually possible using the "debuggable = set false" flag on Android systems, for example;
r) You should directly invoke the application that receives system calls and messages, avoiding the use of resources such as the propagation (broadcast) of intents on Android systems or App Extensions on iPhone systems;
s) The application must implement a standard configuration for the user as safe as possible (seeking a balance between security and usability);
t) The application must inform the user about the possible risks when changing the security parameters in the configuration. In these cases, the default option selected must be the most restrictive from the security point of view;
u) The app should automatically update on devices when needed.

2 Session Management

a) The session ID must meet the following requirements:
   ☒ Changes and is different for each valid user login and authentication;
   ☒ It is removed after the "LogOut" (device unlinking) process.
b) The session must be limited to a maximum of 15 (fifteen) minutes of inactivity;
c) The logout functionality must completely end the session or associated connection;
d) If a session was established before login, then this session must be closed for establishing a new session after login;
e) Encrypted protocols, such as HTTPS/TLS, should be used to protect sensitive data transmitted over the network;
f) Web data trafficked by the application, such as traffic via HTTPS, should not be stored, even in cache files.

3 Data Protection

a) The application must validate the encryption certificates used during data transfer;
b) The application must use TLS for all connections that:
   ☒ Transmit user authentication credentials or session tokens;
   ☒ Send or receive sensitive data or access sensitive operations;
   ☒ Are related to the application administration.
c) c) Sensitive data must not be sent through alternative channels, such as SMS, MMS or notifications;
d) d) The application should not store sensitive data on shared resources of the device, such as shared directories or SD card. For Android systems, the local storage of information on the device must use local file encryption using "setStorageEncryption";
e) e) The application must not store sensitive data in the device local databases. If any data requires storage, it must use protection techniques, such as, e.g.:, truncation. This is true even if sensitive data is stored using encryption techniques, such as iOSKeychain or SQLite bases on Android systems;
f) f) The application must not offer auto-complete for sensitive data, such as passwords, personal or credit card information;
g) g) The application must not allow the export of sensitive activities performed by the application;
h) h) Applications that traffic sensitive data must use Certificate Pinning techniques to prevent the interception of application traffic.

4 4Authentication and Password Management

a) In instances where the mobile application requires a user to create a password or PIN (say, for offline access), the application should never use a PIN, but impose a password that follows a strong password policy;
b) Mobile devices can also offer the possibility to use biometric data to perform authentication, which should never be used due to problems with false positives/negatives;
c) Clear memory locations that contain passwords directly after their hashes have been calculated;
d) Based on the risk level of the mobile app, consider using two-factor authentication;
e) For device authentication, avoid using only any identifier provided by the device (such as UID or MAC address) to identify the device, but take advantage of the specific identifiers of the application, as well as the device (which ideally would not be reversible);
f) In scenarios where offline access to data is required, add an intentional delay of two (2) seconds to the password entry process after each unsuccessful entry attempt;
g) In scenarios where offline access to data is required, account/application and/or application data locking must be performed after ten (1o) invalid password attempts;
h) When using a hashing algorithm, use only an NIST approved standard, such as SHA-2;
i) Always consider including context information (such as IP location etc ...) during the authentication processes to perform the detection of login anomalies;
j) Instead of passwords, use industry-standard authorization tokens (which expire as often as possible) that can be safely stored on the device (according to the OAuth model) and that are limited to the specific service;
k) Integrate a CAPTCHA solution whenever it improves security without disturbing the user experience (such as during new user registrations, posting user comments, online surveys, "get in touch", emailing pages etc.).

5 Code obfuscation

a) Obfuscate all confidential application code by running an automated code obfuscation program using

[Signature]

commercial third party software or open source solutions;

b) For applications that contain confidential data, personal data, sensitive personal data, anti-debugging techniques must be implemented (for example, prevent a debugger/debug from being attached to the process; *android: debuggable = "false"*).

[Signature]