Information and Cybersecurity Policy for Third-Party Contractors

I. INTRODUCTION

The Banrisul's Information and Cybersecurity Policy aims to establish the fundamental guidelines in order to protect Banrisul's and its customers' data and information, as well as their systems and assets. It guides the company to prevent, identify, evaluate, monitor, fight and treat or mitigate the main factors that generate information and cybersecurity risks.

Information security is the guarantee that information will be protected, kept intact and available only to those with the right to access it. Information security disciplines address all types of controls to make this possible, from logical tools such as cryptography and access keys, to physical controls such as access restriction to the datacenter and equipment positioning.

Cybersecurity is the safeguard of people, society, organizations and nations against cyber risks. It is a subset of information security, which addresses more emphatically the logical protection tools.

The following content is presented in form of Principles, and summarizes the main cybersecurity and information security practices to be accomplished by Third-Party contractors, in accordance with our Information and Cybersecurity Policy, approved at a meeting of the Board of Directors on September 10, 2025. These Principles must document and implement mechanisms, processes, procedures and controls to comply with the items in this document, applicable exclusively to their scope of provision of services/object of the contract.

For the purpose of this document, Third-Party contractor is any and all product supplier, service provider, as well as their respective agents and personnel, who have a contract involving the storage, processing or treatment of data or information owned by the companies controlled by Banrisul Group, named in this document as 'Banrisul'.

This document is updated at least annually. Consequently, guidelines contained herein may be modified. Banrisul provides and maintains this updated version to inform Third-Party contractors and their personnel.

II. General Principles for Data and Information Safety

Classification:

The Third-Party contractor must respect the data and information classification defined by Banrisul and, whenever the classification is not available, Banrisul's data and information must be managed as confidential.

The use of Artificial Intelligence solutions with any kind of information owned by Banrisul will only be allowed through formal and express authorization from Banrisul.

Protection:

Data and information owned by Banrisul must be protected since their creation, against unauthorized access, modification, subtraction, destruction or unauthorized disclosure.

To this end, Banrisul recommends the usage of mechanisms that guarantee:

- Confidentiality: appropriate confidentiality preservation mechanisms must be applied for each type of data and information transmitted, processed or stored, preventing its misuse.
- Integrity: appropriate integrity preservation mechanisms must be applied for each type of data and information transmitted, processed or stored, preventing tampering.
- Authenticity: authenticity preservation mechanisms must be applied, adequate for each type of data and information transmitted, processed or stored, guaranteeing its legitimacy and non-repudiation.
- Availability: backup copies of data and information used by critical systems must be kept in protected and managed environments, maintaining availability to their owners in case of need for restoration for a reasonable period of time.
- Traceability: appropriate mechanisms must be applied for each type of data and information to be protected, and traceability information must be kept for a reasonable time, in accordance with audit needs, and in compliance with current legislation.
- Other: stated in the other Principles throughout this Policy.

III. Principles for personnel safety

Safe Hiring of Human Resources:

The Third-Party contractor must have and present the Information and Cybersecurity Policy to its personnel and maintain agreements with them about their roles and responsibilities in information security, in the form of terms, agreements or declarations of confidentiality and secrecy that must be signed by them.

Professional Secrecy:

Third-Party contractor's personnel must maintain absolute professional secrecy, ensuring the protection of Banrisul's data and information to which they have access.

It is not permitted to record work meetings or events, whether physical at Banrisul's headquarters or in corporate videoconferencing systems, unless expressly authorized to do so. Likewise, it is not allowed to record meetings involving Banrisul's contractual matters at Third-Party contractors' premises.

Responsible Usage of Banrisul's Resources:

Third-Party personnel are responsible for the usage of resources, whether technological or not, made available by Banrisul to carry out their duties, in providing services to Banrisul, in accordance with the rules established in the contract.

Passwords used to access the resources are personal, non-transferable and must be chosen and modified in accordance with the best practices guided by Banrisul's Information Security area.

Only original software and equipment are allowed for the data handling of Banrisul's assets.

It is not permitted to disable or uninstall security mechanisms installed by Banrisul in technological resources, without express authorization by the managers of the Banrisul's Technology areas.

It is not allowed to use systems and applications installed locally or that operate online through the Internet that have not been expressly authorized or made available by the managers of the Banrisul's Technology areas.

It is not allowed to send or store Banrisul's data and information via online systems and applications through the Internet or the usage of portable storage media.

It is not permitted the usage of technological resources provided by the Banrisul for personal purposes.

Culture and Awareness:

All personnel hired to work in contracts signed with Banrisul must be aware of and committed to their role in protecting Banrisul's data, information and resources to which they have access, technological or not. It is recommended a periodic evaluation of personnel in relation to the fulfillment of their roles and functions related to information and cybersecurity.

During the contractual period, Banrisul may make available awareness material associated with this or future versions of this Policy. The usage of this material by Third-Party contractors is mandatory.

IV. PRINCIPLES FOR CONDUCTING SAFE BUSINESS

Conception of Safe Products and Services:

All new products and services developed by Third-Party contractors for usage by Banrisul must undergo an evaluation of information and cybersecurity general aspects. The initial assessment must be carried out by the Third-Party contractor and subsequently by the contract manager, in light of the items of this Policy and, if information security issues are identified, Banrisul's Information Security area must be consulted.

Safe Business Environment Maintenance:

All business environments maintained by Third-Party contractors in compliance with contracts with Banrisul, such as service rooms, business rooms, units or administrative areas, must provide continuous protection of the company's data and information by maintaining safe environments for customer service and attendance, conducting business and carrying out administrative and operational activities.

Safe Choice of Business Partners:

The Third-Party contractor must choose and contract business partners capable of complying with this Information and Cybersecurity Policy, in what is applicable. In this sense, the Third-Party contractor must observe, in any contracts involving the provision of services to Banrisul, at least compliance with Principles stated in this document.

V. PRINCIPLES FOR SECURE SOFTWARE DEVELOPMENT

Safe Development:

Systems and applications developed for usage by Banrisul and its customers must be in accordance with the internal standards for system development, IT infrastructure and current information security standards, seeking to protect them in the best possible way from malicious exploitation by threats from any source. The best software

development practices on the market should also be considered. Details on this process can be consulted with Banrisul's Information Security area.

Vulnerability Analysis in Source Codes:

Systems and applications developed for usage by Banrisul and its customers must have their code evaluated on the existence of security vulnerabilities. Details on this process can be consulted with Banrisul's Information Security area.

Safe Tests and Homologations:

Systems and applications for usage by Banrisul and its customers must be developed and tested in logically segregated environments and undergo standardized tests to ensure their functionality and security. Testing must be carried out not only by developers and testers, but also by managers of systems or applications being developed. Details on this process can be consulted with Banrisul's Information Security area.

Secure Deployment:

Methods of code obfuscation and code signing must be applied before the system or application is ready for deployment.

The implementation of a system or application must always apply the Change Management principle, with the approval of all areas eventually affected by this implementation, except for extraordinary situations in which the business continuity is at risk.

In the first implementation of a system or application involving Banrisul’s data or information, there must be guarantee that the security of this system or application has been evaluated in the light of this Policy. This assessment also applies to the implementation of improvements that significantly change the security of a system or application already in production.

VI. Principles for Technological Environment Security

Physical Protection:

The Third-Party contractor's datacenters must be physically segregated from the rest of its facilities, and physical access control mechanisms must be in place to ensure the protection of infrastructure assets that support the Banrisul's systems and applications against unauthorized physical access. Other technology environments that exist outside of datacenters and require physical protection, such as vault rooms, must be given the level of physical protection appropriate to the sensitivity of the data and information they are protecting.

Logical Protection:

The internal logical networks (accessible only internally) and external (accessible through the Internet) must be logically segregated at the lowest level of granularity that is technically possible, using perimeter protection mechanisms that guarantee the protection of the technological environment from unauthorized logical access.

Authentication and Access Management:

Access management is based on the least privilege principle, that is, all access to technology equipment, logical storage areas, systems and applications that make up the computing environment must be granted under justified need and only during the necessary time, according to the individual's role within the process and respecting the appropriate segregation of duties. Access must be reviewed periodically by the managers responsible for granting it.

All access to technology assets and internal and external systems must be authenticated, and the usage of passwords and authentication methods must follow the standards defined by the Banrisul’s Information Security area.

Whenever the technology (hardware) or programming method used (software) supports this, access to systems and applications must be performed using multi-factor authentication methods, as well, when applicable, single sign-

on mechanisms linked to the Banrisul's access management system. Details on this process can be consulted with Banrisul's Information Security area.

Usage of Cryptography and Digital Certification:

The protection of data and information is largely based on the usage of cryptography and digital certification. The Third-Party contractor must apply strong cryptography and digital certification techniques defined by Banrisul's Information Security area, both in the development of systems and applications and in the configuration of databases and equipment that carry out the transmission or storage of this data and information.

Safe Adoption of Technologies:

It is recommended that every project for the adoption of any technology by the Third-Party contractor to serve Banrisul undergo an assessment of information and cybersecurity general aspects. The initial assessment must be carried out by the Third-Party contractor together with the contract manager in light of the items in this Policy and, if information security issues are identified, Banrisul's Information Security area must be involved.

Protection Against Malicious Software:

The Third-Party contractor must adopt mechanisms for detection and removal of malicious software for all technology assets in which this measure is applicable to prevent and give visibility to possible attempts to install malicious software by threat agents.

Vulnerability Management:

The Third-Party contractor must maintain strategies and carry out preventive actions that allow the management of vulnerabilities in its technological environment. Details on this process can be consulted with Banrisul's Information Security area.

Intrusions Prevention, Detection and Containment:

The Third-Party contractor must implement intrusion prevention and detection mechanisms in the perimeters of its logical environment, as well as in strategic points of the internal and external networks, with the purpose of preventing and giving visibility to eventual malicious exploitation attempts by intrusion agents. Details on this process can be consulted with Banrisul's Information Security area.

Environment Monitoring:

The Third-Party contractor must constantly monitor its environment, aiming to identify possible information and cybersecurity incidents that may be occurring or about to occur. This monitoring must indicate, to some extent, the effectiveness of the security mechanisms implemented by the Third-Party contractor. Details on this process can be consulted with Banrisul's Information Security area.

Incident Handling:

The recording and treatment of information and cybersecurity incidents must occur according to their relevance. The Third-Party contractor must share with Banrisul information regarding information and cybersecurity incidents that involve the provision of the service object of the contract between the two companies. Details on this process can be consulted with Banrisul's Information Security area.

Change Management:

The Third-Party contractor must have a change management process in line with the best practices on the market, in order to ensure that the implementation of changes in systems, applications and infrastructure assets does not affect their availability or the confidentiality and integrity of Banrisul’s data and information.

Disaster Recovery:

The Third-Party contractor's computing environments must be maintained in physical and logical configurations that seek to minimize product or service interruptions caused by unavailability of assets, systems or applications.

The Third-Party contractor must ensure that the return time of the asset or system is always within the acceptable limit, using disaster recovery mechanisms so as not to jeopardize the continuity of service provision for Banrisul.

Tests of Disaster Recovery Plans must foresee scenarios of cyber incidents when applicable. Details on this process can be consulted with Banrisul's Information Security area.

VII. ADDITIONAL INFORMATION

Additional details or clarifications on this document can be consulted with the contract manager.

This document was last updated on December 17, 2024.

banrisul

INFORMATION TECHNOLOGY SECURITY UNIT