Crown Digital:

Information Security and Cybersecurity Policy

CROWN

TECHNICAL SHEET:

TITLE: Information Security and Cybersecurity Policy ("Policy")

RESPONSIBLE DEPARTMENT: Risk and Compliance

RESPONSIBLE DIRECTOR: Head of Risk and Compliance

POLICY DESCRIPTION: This Policy establishes the principles, guidelines, responsibilities, and controls for managing information security and cybersecurity at Crown, in compliance with applicable regulations and best market practices, aiming to protect the information assets of the company, its clients, and partners.

APPLICATION: To Crown Digital, all its subsidiaries, employees, directors, board members, interns, service providers, consultants, and any third parties who have access to Crown's information or systems.

APPROVED BY: Board of Directors

VERSION	PUBLICATION	DESCRIPTION OF CHANGES
1.0	17/04/2025	Policy creation (initial version).

CROWN

ÍNDICE

PART I – INFORMATION SECURITY POLICY

1. Introduction and Objectives

This Information Security and Cybersecurity Policy ("Policy") establishes the foundations for the protection of informational assets in the possession, custody, or ownership of CROWN SOCIEDADE PRESTADORA DE SERVIÇOS DE ATIVOS VIRTUAIS LTDA (“Crown”).

Its fundamental purpose is to ensure the Confidentiality, Integrity, and Availability (CIA Triad) of all information processed, stored, and transmitted by the company, its systems, and its partners.

This document formalizes Crown's commitment to security, establishing a robust governance and control structure.

This structure was proactively designed, anticipating the high standards of security and diligence expected for obtaining and maintaining the future VASP license with the BACEN.

The Policy is, therefore, based on the guidelines of the Brazilian legal framework for the sector, notably Law No. 14,478/2022, and adopts as a reference the best practices and prudential cybersecurity requirements applicable to the financial ecosystem, such as those stipulated in CMN Resolution No. 4,893/2021.

The applicability of these guidelines is universal within the Crown ecosystem, being mandatory for all employees (regardless of their hiring regime), directors, board members, interns, consultants, and any third-party service providers who, in the exercise of their functions, have access to the company's information assets or systems.

Adherence to this Policy is a condition for the initiation and maintenance of any relationship with Crown.

As a formalization of this commitment, all individuals covered by this Policy must sign the Term of Responsibility and Confidentiality (Annex I) at the beginning of their relationship with the company.

Crown's Senior Management recognizes information security and cybersecurity as critical and essential functions for protecting client assets, maintaining market trust,

and ensuring the sustainability of operations.

The Executive Board is committed to providing the necessary financial, human, and technological resources for the effective implementation, maintenance, and continuous improvement of the controls and processes described herein, promoting a culture of security at all levels of the organization.

This policy will be reviewed and updated at least annually or whenever significant changes occur in the threat landscape, business operations, technological infrastructure, or regulatory framework, as determined by the Cybersecurity Committee.

This continuous review process is a pillar of Crown's governance and demonstrates the company's commitment to the continuous improvement of its security posture, a fundamental requirement for institutions regulated by the Central Bank of Brazil (BACEN).

2. Information Classification and Handling

The application of effective and risk-proportional security controls depends on a clear understanding of the sensitivity and criticality of the data.

Crown adopts a formal information classification system to ensure that the most valuable assets receive the highest level of protection, optimizing resource allocation and guiding security actions at all levels of the organization.

The classification of an information asset determines its handling, storage, transmission, and disposal requirements.

Adapting a standard classification model is essential to reflect the unique and high-impact assets of a VASP.

Unlike a traditional company, where strategic plans might be the most critical asset, in a VASP, cryptographic materials and access credentials directly control monetary value.

Therefore, the policy must be granular and specific. By explicitly defining API keys, infrastructure secrets, and cryptographic key shares as 'Restricted', Crown imposes the highest level of control over them, directly linking the classification scheme to the mitigation of its greatest operational and financial risks.

All information produced, received, or managed by Crown must be classified into one of the following four categories:

- **Public:** Information created for the purpose of external disclosure, with no access restrictions. Its disclosure does not cause harm to Crown, its clients, or partners. Examples include approved marketing materials, press releases, and the content of the company's public website.
- **Internal Use:** Information intended for general circulation among Crown employees, but not for the external public. Its unauthorized disclosure could cause minor operational disruptions or embarrassment, but without significant financial, legal, or reputational impact. Examples include non-sensitive internal policies, general procedure manuals, and internal communications.
- **Confidential:** Information of a sensitive nature, access to which must be restricted to specific groups of employees based on the "need-to-know" principle. The unauthorized disclosure of this information could result in operational, financial, or reputational damage to Crown, its clients, or partners. Examples include business plans, internal financial information, employee personal data (HR), contracts with partners, and strategic discussions.
- **Restricted:** The highest level of classification, reserved for Crown's most critical and sensitive information assets. Access is strictly controlled, monitored, and limited to the minimum number of authorized individuals, often requiring multi-party approvals. The unauthorized disclosure, alteration, or unavailability of this information could cause severe and irreparable damage, including massive financial losses, serious regulatory violations, loss of client funds, and catastrophic damage to the company's reputation. Examples include:
    - API keys from banking, custody, and cloud infrastructure partners.
    - Private keys or Multi-Party Computation (MPC) key shares used in the custody of virtual assets.
    - Access credentials with administrator privileges to critical systems (AWS, Google Workspace, custody platforms).
    - Customer identification data (KYC/AML) and detailed transaction history.
    - Trade secrets, proprietary algorithms, and source code of critical applications.
    - Unremediated penetration test reports and vulnerability analyses.

The following table details the handling requirements for each classification level, serving as a practical guide for all employees and automated systems.

Table 1: Information Classification and Handling Matrix

Classification Level	Description	Examples (at Crown)	Access Requirements	Encryption Requirements (Rest/Transit)	Sharing Rules
Public	Information for external disclosure.	"Marketing materials, public website."	Unrestricted access.	Not required.	Freely permitted.
Internal Use	Information for all employees.	"Internal communications, procedure manuals."	Access by all Crown employees.	Mandatory in transit (e.g., TLS).	Internal to Crown. External sharing prohibited.
Confidential	Sensitive information for specific groups.	"Business plans, HR data, financial information."	"Access restricted by role (RBAC) and ""need-to-know""."	"Mandatory at rest and in transit (e.g., disk encryption, AWS KMS, TLS)."	Controlled via access groups. External sharing only with NDA and encryption.
Restricted	Critical information with minimal access.	"API keys (banking, custody), customer KYC data, MPC key shares."	"Strictly controlled access, with approval quorum and intensive monitoring."	Strong encryption mandatory at rest (e.g., AWS KMS) and in transit (e.g., TLS 1.2+).	Sharing prohibited by default. Exceptions require formal approval from the Risk and Compliance Committee.

3. Information Lifecycle Management

Information security must be applied throughout all phases of its existence, from creation to final disposal. Crown establishes rigorous controls for each stage of the data lifecycle to ensure regulatory compliance and continuous protection.

3.1 Collection and Generation

All data collection, especially of personal customer data for KYC/AML processes, must be carried out lawfully, fairly, and transparently, for legitimate and specific purposes. Crown strictly adheres to the principle of data minimization, ensuring that the amount of information collected is limited to what is strictly necessary for the stated purpose, in full compliance with the General Data Protection Law (LGPD, Law No. 13,709/2018).

3.2 Storage and Backup

Secure storage is a pillar of data protection. All data classified as 'Confidential' or 'Restricted' must be stored in encrypted format, both at rest and in transit. For Crown's infrastructure, this translates into mandatory technical requirements:

- **AWS Infrastructure:** Data stored in databases (Amazon RDS) must use encryption with keys managed by the AWS Key Management Service (KMS). Data in Amazon S3 buckets must, by default, be encrypted on the server-side (Server-Side Encryption), preferably with KMS-managed keys (SSE-KMS) to allow for granular access control.

- **Collaboration Environment (Google Workspace):** Access to files classified as 'Confidential' or 'Restricted' in Google Drive must be strictly limited to specific access groups. Data Loss Prevention (DLP) policies must be applied to monitor and prevent the improper storage or sharing of sensitive information.

Crown maintains a robust backup policy to ensure operational resilience and disaster recovery capability. All backups of critical data, especially those containing 'Restricted' information, must be encrypted. Backups will be stored in an AWS geographic region distinct from the production region to ensure recovery in the event of a complete regional failure. Backup restoration procedures will be tested periodically, at least annually, to validate their effectiveness and adequacy.

3.3 Retention

Crown will comply with all legal and regulatory deadlines for record retention. In accordance with the requirements of BACEN and COAF for financial institutions and VASPs, all transaction records, customer identification data (KYC), and relevant communications will be kept for a minimum period of 5 (five) years from the completion of the transaction or the end of the client relationship. This period may be extended if determined by specific legislation or court order. A formal data retention schedule will be maintained and reviewed annually by the Risk and Compliance area.

3.4 Secure Information Disposal

At the end of the legal retention period or the useful life of the information, the data must be disposed of in a secure and irrecoverable manner to prevent unauthorized disclosure. The method used will depend on the media and the classification of the information:

- **Clear:** Overwriting data on digital media using specialized software that prevents recovery by simple tools. Applicable to 'Internal Use' information.
- **Purge:** Using techniques such as degaussing (demagnetization) for magnetic media or cryptographic overwriting, making data recovery technically infeasible. Applicable to 'Confidential' information.
- **Destroy:** Physical disintegration of the media through shredding, pulverization, melting, or incineration. This is the mandatory method for any physical media (HDDs, SSDs, flash drives, paper) that has stored information classified as 'Restricted'.

For all media disposal, a formal record will be maintained, documenting what was disposed of, the date, the method used, and, if applicable, the third-party company responsible for the service, ensuring a complete audit trail.

PART II – CYBERSECURITY POLICY

4. Cybersecurity Governance

Crown's cybersecurity governance is the system by which the company directs and controls its security activities, aligning them with business objectives, risk appetite, and strict regulatory requirements. The following structure is designed to directly meet the requirements of BACEN's CMN Resolution No. 4,893, demonstrating a commitment to maturity and responsibility in cyber risk management.

4.1 Structure of Responsibilities (Aligned with CMN Resolution No. 4,893)

A clear and well-defined governance structure is fundamental to the effectiveness of the security program. BACEN's regulation requires the appointment of a director responsible for the policy but does not mandate the creation of a specific role such as a Chief Information Security Officer (CISO). Crown's approach is to integrate this function into its existing governance structure, ensuring regulatory compliance without inflating the organizational structure. This approach demonstrates a mature understanding that security is a business risk function, not just a technical issue.

- **Executive Board:** It is the highest level of accountability for cybersecurity. It is responsible for approving this Policy, ensuring the allocation of necessary resources for its implementation, and promoting a security culture throughout the organization.
- **Responsible for Cybersecurity:** In compliance with Art. 4 of CMN Resolution No. 4,893, Crown formally designates the **Director of Risk and Compliance** as the statutory officer responsible for the Cybersecurity Policy and its implementation. Their duties include:
    - Proposing, implementing, and ensuring the application of this Policy and its associated procedures.
    - Leading the Risk and Compliance Committee in its deliberations on cybersecurity.
    - Supervising the cyber risk management process and periodically reporting the security status and residual risks to the Executive Board.
    - Coordinating the response to cybersecurity incidents.

    - Managing the security awareness and training program.

- **Risk and Compliance Committee:** This existing committee will also act as the Cybersecurity Committee, being the governance forum responsible for the supervision and deliberation on security strategies and issues.

    - **Composition:** Chaired by the Director of Risk and Compliance and composed of representatives from the Technology, Operations, and Legal departments.
    - **Frequency:** Ordinary quarterly meetings and extraordinary meetings whenever necessary.
    - **Formalization:** All meetings will be documented through minutes, which record the deliberations and decisions made. The minutes will be securely filed and available for internal and external audit.

- Technology Department: This is the executing area responsible for implementing, configuring, maintaining, and monitoring the technical security controls defined in this Policy on Crown's systems, networks, applications, and infrastructure.

- All Employees: Each employee is responsible for understanding and adhering to this Policy in their daily activities, protecting the company's information and assets, and immediately reporting any anomalies or security incidents.

To eliminate ambiguities and formalize this structure, the following Responsibility Assignment Matrix (RACI) defines the roles for key security processes. A RACI matrix is a standard governance tool that demonstrates to auditors and regulators that Crown has mature and well-defined processes.

Table 4: Security Responsibility Matrix (RACI)

Process / Activity	Executive Board	Director of Risk and Compliance	Risk and Compliance Committee	Technology	Legal
Policy Approval and Review	A	R	C	C	C
Cyber Risk Management	I	A	R	C	C
Critical Incident Response	A	R	C	R	C
Access Granting/Review	I	A	I	R	I
Third-Party Security Due Diligence	I	A	C	C	R
Implementation of Technical Controls	I	I	C	R	I
Training and Awareness	I	A	C	I	R
Communication to BACEN	A	R	C	I	C

Key: R (Responsible), A (Accountable), C (Consulted), I (Informed)

5. Cyber Risk Management

Crown adopts a formal, continuous, and documented cyber risk management process to identify, analyze, evaluate, and treat threats to its operation. This process is conducted in accordance with market best practices and the requirements of CMN Resolution No. 4,893. The risk assessment will be performed at least annually or whenever significant changes occur in the business, technological, or regulatory environment.

The assessment methodology will consider threat sources, existing vulnerabilities in the infrastructure and processes, the likelihood of an adverse event, and the potential impact across multiple dimensions: financial, operational, reputational, and regulatory.

The risk assessment process will consider, but is not limited to, the following threats and attack vectors specific to the VASP ecosystem:

- **Compromise of Credentials and API Keys:** Theft of API keys from banking partners or the custody platform, allowing for unauthorized movement of funds.
- **Smart Contract Attacks:** Exploitation of code vulnerabilities in smart contracts deployed on blockchain networks (e.g., re-entrancy attacks, integer overflow/underflow, business logic flaws) aiming to divert funds.
- **Social Engineering and Phishing:** Attempts to deceive employees into revealing access credentials to critical systems or approving fraudulent transactions.
- **Cloud Infrastructure Attacks (Cloud):** Exploitation of misconfigurations in AWS services, such as public S3 buckets, permissive Security Groups, or weak IAM policies, to gain unauthorized access to infrastructure and data.
- **Insider Threats:** Malicious or negligent actions by employees with privileged access, such as the improper approval of transactions on the custody platform, exfiltration of customer data, or introduction of malicious code.
- **Supply Chain Attacks:** Compromise of a software or third-party service provider, using their legitimate access to attack Crown's infrastructure.

For each risk identified and assessed as being above the risk appetite defined by the Board, one or more of the following treatment strategies will be formally defined and documented:

- **Mitigate:** Apply security controls to reduce the likelihood or impact of the risk. This is Crown's primary strategy.
- **Accept:** For low-impact and low-probability risks, the Board may decide to formally accept the risk, documenting the justification and acceptable loss levels.
- **Transfer:** Transfer part of the financial impact of the risk to a third party, primarily

through the purchase of cyber insurance policies.
- **Avoid:** Change business processes, technologies, or architectures to eliminate the activity that gives rise to the risk.

6. Security Controls for Critical Infrastructure and Operations

This section details the mandatory security controls for the technological components that support Crown's operations. These controls translate security principles into specific, auditable technical requirements, demonstrating technical competence to the regulator.

6.1 Secure Management of Critical Service Credentials

The API keys and other credentials that connect Crown to its banking partners and custody services are the company's most critical assets, as they directly control the flow of value. Their management must follow the most rigorous security practices.

- **Classification and Storage:** All API keys, authentication tokens, and other critical service credentials are classified as 'Restricted'. It is strictly prohibited to store these secrets in source code, configuration files, environment variables on workstations, or in any code repository (e.g., Git). The only permitted storage location for these secrets is a centralized and secure secret management service (secrets vault), such as **AWS Secrets Manager**.
- **Access Control:** Programmatic access to stored secrets must be granted exclusively through machine identity mechanisms with temporary credentials (e.g., IAM Roles), which provide them to AWS services (such as EC2 instances or Lambda functions) that need the secret at runtime. The permission policies associated with these identities must follow the principle of least privilege. Direct user access to these secrets is prohibited by default and requires exceptional justification and approval.
- **Rotation Policy:** It is mandatory that all API keys and critical credentials be rotated periodically to limit the window of opportunity in case of a compromise. Crown establishes a maximum lifecycle of **90 days** for any critical API key. Rotation should preferably be automated using the native features of the secret management service.
- **Monitoring and Alerting:** All API calls to the secret management service, successful or not, must be logged in AWS CloudTrail for auditing and investigation purposes. Automatic alerts must be configured in Amazon CloudWatch to immediately notify the Risk and Compliance team of suspicious security events.

6.2 Cloud Infrastructure Security (AWS)

Crown's AWS infrastructure is the backbone of its operations. Its security follows the best practices of the AWS Well-Architected Framework, focusing on resilience, security, and compliance, aligned with expectations for financial services.

- **Network Security:** The network architecture is based on Virtual Private Clouds (VPCs) with strict segmentation between public and private subnets. Traffic is controlled by Network ACLs (NACLs) and Security Groups configured with least-privilege rules, allowing only strictly necessary traffic.
- **Application Protection:** Web applications exposed to the internet are mandatorily protected by **AWS WAF (Web Application Firewall)** to mitigate common threats and by **AWS Shield** for protection against denial-of-service (DDoS) attacks.
- **Security Monitoring: Amazon GuardDuty** is enabled in all accounts for intelligent threat detection. **AWS Config** is used to continuously monitor the configuration compliance of resources with Crown's security policies, generating alerts for deviations.

6.3 Security in the Custody and Transaction of Virtual Assets

The security of the custody platform is paramount. Crown adopts robust technical and operational controls to protect client assets.

- **Custody Architecture:** The custody of virtual assets must, mandatorily, be performed using technology that eliminates single points of failure, such as **Multi-Party Computation (MPC)** or **Hardware Security Modules (HSMs)**. This model eliminates the single point of failure of a traditional private key because the key never exists in its entirety in a single location. Signing transactions requires the participation of a quorum of parties, making the theft of a single "share" of the key useless to an attacker.
- **Transaction Governance (Policy Engine):** Automating governance via a transaction policy engine is a critical and non-bypassable control. These rules are the heart of Crown's operational security. The table below details the mandatory rules, which demonstrate to regulators a sophisticated and automated governance system, going beyond mere manual procedures.

Table 3: Mandatory Transaction Policy Engine Rules Table

Transaction Scenario	Example Rule	Trigger Parameters (Asset, Value, Destination)	Approval Requirement	Risk Justification
Client Withdrawal (Retail)	Allow withdrawals to whitelisted addresses with approval from 1 member of the "Operations" group.	Asset: BTC, ETH, etc. | Value: < $10,000 USD | Destination: Whitelisted Address	1 of N from Operations group	Mitigates operational error and internal fraud in low-value transactions, while maintaining agility.
Client Withdrawal (High Value)	Require approval from 2 members of different groups for high-value withdrawals.	Asset: * | Value: >= $10,000 USD | Destination: Whitelisted Address	1 of N from Operations group + 1 of N from Risk and Compliance group	Prevents high-impact internal and external fraud through segregation of duties and the "four-eyes" principle.
Transfer to New Address	Block direct transfers to non-whitelisted addresses. The whitelisting process requires approval from 2 administrators.	Asset: * | Value: * | Destination: NON-Whitelisted Address	Action: BLOCK	Prevents diversion of funds to attacker addresses or addresses entered by mistake (fat-finger errors). The control is in the whitelisting process.
Treasury Rebalancing	Allow transfers between internal wallets (Vaults) with approval from 1 member of the "Treasury" group.	Asset: * | Value: * | Origin/Destination: VAULT_ACCOUNT	1 of N from Treasury group	Streamlines internal liquidity management operations, which have a lower risk of external fund loss.
Interaction with DeFi Contract	Require approval from 2 members, including 1 from the "Risk and Compliance" group, for any call to a smart contract.	Operation: CONTRACT_CALL | Destination: Contract Address	1 of N from Treasury group + 1 of N from Risk and Compliance group	Mitigates the risk of interacting with malicious or vulnerable smart contracts, ensuring a risk analysis before execution.

7. Third-Party Security

CMN Resolution No. 4,893 establishes rigorous requirements for contracting data processing and storage services, especially in the cloud, recognizing that the supply chain is an extension of the institution's attack surface. Crown adopts a formal process to ensure that its partners and suppliers meet the same high security standards that the company applies internally.

Before contracting any third-party service that will access, process, or store information classified as 'Confidential' or 'Restricted', or that is considered critical to the operation (such as cloud providers, collaboration platforms, or custody platforms), the Risk and Compliance area will conduct a security due diligence process. This process will use the questionnaire detailed in **Annex II – Third-Party Security Due Diligence Model**, which assesses the maturity of the supplier's policies, their certifications (e.g., ISO 27001, SOC 2 Type II), incident management processes, and ability to meet the regulatory requirements applicable to Crown.

All contracts with critical service providers must contain specific information security clauses that address, at a minimum: the supplier's obligation to protect Crown's data, a clear definition of responsibilities in the event of a security incident, including notification deadlines, Crown's right to audit the supplier's controls, and liability clauses in case of breaches. The security posture of critical suppliers will be reassessed annually.

8. Monitoring, Testing, and Resilience

A static security posture is insufficient. Crown implements a continuous monitoring and testing program to validate the effectiveness of its controls and ensure its resilience against attacks.

- Crown will implement a **SIEM (Security Information and Event Management)** solution to centralize, correlate, and analyze security logs from all its critical sources: AWS (CloudTrail, GuardDuty), Google Workspace, custody platforms, and network systems. The SIEM will be configured with rules to detect attack patterns and generate real-time alerts for the Risk and Compliance team.
- To proactively validate the effectiveness of controls, Crown will conduct the following security tests:
    - **Penetration Tests (Pen Tests):** At least annually, a qualified external company will be hired to conduct penetration tests on the external infrastructure (web applications, APIs).

- **Vulnerability Scanning:** Automated vulnerability scans will be performed continuously on cloud environments and endpoints to identify known flaws.
- **Social Engineering Tests:** Simulated phishing campaigns will be periodically sent to employees to test and reinforce awareness.

9. Cyber Incident Response Plan

A detailed, documented, and tested Cyber Incident Response Plan (CIRP) is a fundamental requirement of CMN Resolution No. 4,893 and good governance. Crown's plan is based on market frameworks like NIST and includes the phases of Preparation, Detection and Analysis, Containment, Eradication, Recovery, and Lessons Learned. The plan formally defines the Incident Response Team (CSIRT), led by the Head of Cybersecurity (Director of Risk and Compliance), and includes specific playbooks for Crown's highest-risk scenarios, such as "Banking API Key Compromise" or "Smart Contract Vulnerability Exploit." A post-mortem report is mandatory after every significant incident to ensure learning and continuous improvement.

9.1 Communication of Relevant Incidents to BACEN

This section is of critical importance for regulatory compliance. Crown's CIRP includes a specific procedure for assessing the relevance of security incidents, in accordance with the criteria established by BACEN's regulation for the institutions it supervises. If an incident is classified as relevant, the formal communication process to the regulator will be initiated immediately. In anticipation of specific regulation for VASPs, Crown adopts a conservative stance: when in doubt about relevance, the presumption will be in favor of communication, after consulting with legal counsel, as a demonstration of transparency and cooperation with the ecosystem.

10. Continuous Awareness and Training Program

Crown recognizes that technology alone is insufficient to ensure security. The human factor is a critical component of defense, potentially being the weakest link or the first line of detection. Therefore, the company will maintain a continuous and mandatory security awareness and training program for all employees.

The program will include:

- **Onboarding Training:** All new employees will receive comprehensive training on this Policy, key cyber threats (phishing, social engineering), their security responsibilities, and the safe use of corporate tools.
- **Annual Refresher Training:** All employees must complete an annual update training, covering policy changes, new threats, and lessons learned from recent

market incidents.

- **Continuous Communications:** Security alerts, tips, and newsletters will be distributed regularly to keep security top-of-mind for employees.

11. Sanctions and Disciplinary Measures

The violation of any guideline established in this Policy is considered a serious offense and will not be tolerated. Failure to comply with the rules described herein will subject the offender (whether an employee, service provider, or third party) to disciplinary measures, which will be applied in proportion to the severity of the violation and its impact.

Measures may range from formal warnings and suspension to termination of the employment contract for just cause, under the terms of Art. 482 of the Consolidation of Labor Laws (CLT), or termination of the service agreement. Such measures will be applied without prejudice to applicable civil and criminal penalties under the law. Crown will cooperate fully with the competent authorities in any investigation arising from a violation of this Policy.

Annex I – Term of Responsibility and Confidentiality

Through this instrument, I, **[Employee's Full Name]**, [Nationality], [Marital Status], [Profession], holder of ID card No. and registered with the CPF/ME under No. [CPF Number], hereinafter referred to as **EMPLOYEE**, and **CROWN SOCIEDADE PRESTADORA DE SERVIÇOS DE ATIVOS VIRTUAIS LTDA**, a private legal entity, registered with the CNPJ/ME under No. 59.386.340/0001-45, headquartered at R Caio Prado, 30 Conj 4 Sala 1-A 01303000 Consolacao Sao Paulo SP, hereinafter referred to as **CROWN**, resolve, for the purpose of preserving the personal and professional information of clients and of CROWN, to enter into this Term of Responsibility and Confidentiality ("Term"), which shall be governed by the following clauses, being an integral and inseparable part of the employment or service agreement signed between the parties.

1. Confidential Information
1.1. For the purposes of this Term, any and all information, in any format (written, verbal, digital, tangible, or intangible), that is not in the public domain, to which the EMPLOYEE has access as a result of their relationship with CROWN, is considered Confidential Information. This includes, but is not limited to:
a) Information about clients, including, but not limited to, registration data (KYC), balances, statements, positions, transaction history, and public keys.
b) Information about CROWN's operations, such as business strategies, structured operations, custody structures, API keys, passwords, security policies, business plans, financial data, list of clients, counterparties, suppliers, and service providers.
c) Know-how, techniques, models, diagrams, computer programs (source and executable code), databases, and any other intellectual property of CROWN.
d) Any information classified as 'Internal Use', 'Confidential', or 'Restricted' under the terms of CROWN's Information Security and Cybersecurity Policy.
1.2. Information that: (i) was already in the public domain at the time it was obtained by the EMPLOYEE; (ii) became public domain without the disclosure being in violation of this Term; (iii) was legally disclosed to the EMPLOYEE by third parties who were not under an obligation of confidentiality; or (iv) whose disclosure is required by law or by court order or competent authority, shall not be considered Confidential Information. In the latter case, the EMPLOYEE must immediately notify the Director of Risk and Compliance of CROWN so that appropriate legal measures can be taken.
2. Employee's Obligations
2.1. The EMPLOYEE undertakes to use the Confidential Information strictly and exclusively for the performance of their activities at CROWN, and is prohibited from using, disclosing, copying, reproducing, or in any way making such information known to any third parties, including spouse, relatives, or persons in their close circle.
2.2. The EMPLOYEE is obliged to maintain absolute secrecy regarding the Confidential Information throughout the term of their contract with CROWN and for an indefinite period after its termination.

2.3. The EMPLOYEE acknowledges that all documents, files, systems, and materials prepared or obtained by them in the exercise of their duties are the exclusive property of CROWN and must be returned in full to the company upon termination of their contract, and the maintenance of any copies is prohibited.
2.4. The EMPLOYEE undertakes to fully comply with CROWN's Information Security and Cybersecurity Policy and all its related policies.
3. Consequences of Violation
3.1. The violation of any clause of this Term will be considered a serious offense, leading to the termination of the employment contract for just cause, under the terms of article 482 of the Consolidation of Labor Laws (CLT), or the termination of the service agreement, without prejudice to the determination of liability in the civil and criminal spheres.
3.2. The EMPLOYEE acknowledges that the unauthorized disclosure of Confidential Information may cause irreparable damage to CROWN and its clients, and is obliged to indemnify CROWN for all losses and damages, including lost profits, that may be determined as a result of their violation.
3.3. The EMPLOYEE expressly authorizes CROWN, under the terms of §1 of article 462 of the CLT, to deduct from their severance payments and wages the amounts corresponding to the damages caused by them willfully, up to the legal limit, without prejudice to CROWN's right to seek full compensation for the damage through legal action.
4. Final Provisions
4.1. This Term is an integral part of the rules governing the EMPLOYEE's employment and/or service relationship with CROWN. By signing it, the EMPLOYEE declares to have read, understood, and expressly accepted all its terms and conditions.
And, in agreement, they sign this Term in 2 (two) copies of equal content and form.

[Place], [Month] [Day], [Year].

EMPLOYEE
(Name and CPF)
CROWN SOCIEDADE PRESTADORA DE SERVIÇOS DE ATIVOS VIRTUAIS LTDA
(Legal Representative)

Annex II – Third-Party Security Due Diligence Model

This questionnaire represents the minimum content to be verified in the cybersecurity due diligence process for contracting third parties who will provide critical services or have access to Crown's sensitive information.

Section 1: Governance and Security Policies

- Does the company have a formal, documented Information Security and Cybersecurity Policy approved by senior management? (Request a copy of the document or an executive summary).
- Is the policy reviewed and updated periodically (at least annually)? What is the date of the last revision?
- Does the company have recognized security certifications (e.g., ISO 27001, SOC 2 Type II, PCI DSS)? (Request copies of the certificates/reports).
- Has the company formally appointed a person responsible for information security (CISO or equivalent position)?

Section 2: Risk and Incident Management

- Does the company have a formal cybersecurity risk management process?
- Does the company have a documented and tested Cyber Security Incident Response Plan?
- What is the procedure and contractual deadline for notifying Crown in the event of a security incident affecting Crown's data or services?
- Does the company have a Business Continuity and Disaster Recovery Plan? Is it tested periodically?

Section 3: Technical and Operational Controls

- Describe the security controls for protecting data at rest and in transit (e.g., encryption, algorithms used, key management).
- How does the company manage access to its systems (e.g., password policy, MFA, principle of least privilege)?
- Does the company conduct vulnerability assessments and penetration tests on its infrastructure? How often? (Request a summary of the last test).
- (For cloud services) Describe the specific security controls for the cloud environment (e.g., VPC/VNet configuration, IAM, monitoring, workload protection).
- (For custody/blockchain services) Describe the custody architecture (e.g., MPC, HSM) and the operational controls for transaction authorization.
- (For software/smart contract development) Describe the secure software development lifecycle (SSDLC) and the code audit requirements.

Section 4: Personnel Security and Awareness

- Does the company conduct background checks for employees in sensitive positions?
- Does the company have a security awareness and training program for all its employees? How often does it occur?

Section 5: Regulatory Compliance

- To which data protection and security regulations is the company subject (e.g., LGPD, GDPR)?
- Does the company have controls in place to ensure compliance with the requirements of BACEN's CMN Resolution No. 4,893, regarding the provision of services to regulated institutions?

Annex III – Glossary

- **AWS (Amazon Web Services):** Amazon's cloud computing platform, used by Crown to host its IT infrastructure.
- **BACEN:** Central Bank of Brazil, the regulatory body for the National Financial System and VASPs in Brazil.
- **CIA (Confidentiality, Integrity, Availability):** The fundamental triad of information security.
- **COAF:** Council for Financial Activities Control.
- **DLP (Data Loss Prevention):** Technology or process to prevent the leakage of sensitive data.
- **IAM (Identity and Access Management):** A framework of policies and technologies from AWS to ensure that the right identities have appropriate access to technological resources.
- **KMS (Key Management Service):** An AWS service for creating and managing encryption keys.
- **LGPD:** General Personal Data Protection Law (Law No. 13,709/2018).
- **MFA (Multi-Factor Authentication):** An authentication method that requires more than one form of verification to prove the user's identity.
- **Transaction Policy Engine:** A software system that applies predefined business and security rules to approve, reject, or escalate financial or virtual asset transactions automatically.
- **MPC (Multi-Party Computation):** A field of cryptography that allows multiple parties to jointly compute a function over their private inputs without revealing those inputs. Used in custody solutions to protect private keys.
- **NIST:** National Institute of Standards and Technology, a U.S. government agency that develops technology standards and guidelines.
- **Institutional Custody Platform:** An institutional-grade service or technology for the movement, storage, and issuance of digital assets.
- **RACI:** Responsibility Assignment Matrix (Responsible, Accountable, Consulted, Informed).
- **RBAC (Role-Based Access Control):** An access control model based on the roles of users within an organization.
- **SIEM (Security Information and Event Management):** A software solution that aggregates and analyzes security logs from various sources to provide threat detection and incident response.
- **VASP (Virtual Asset Service Provider):** A term used by the FATF and adopted by Brazilian legislation to designate companies like Crown.
- **VPC (Virtual Private Cloud):** A logically isolated section of the AWS cloud where

Crown's resources are deployed.

- **WAF (Web Application Firewall):** A firewall that filters, monitors, and blocks HTTP traffic to and from a web application, protecting it against attacks.