General principles of IT security

1. Introduction **1**
- 1.1. Preamble and objectives 1
- 1.2. Scope 2
- 1.3. Principles & references 3

2. Safety principles and rules **3**
- 2.1. Reference documents 3
- 2.2. Key measures implemented 4
  - 2.2.1. General measures and governance 4
  - 2.2.2. At Human Resources level 5
  - 2.2.3. At the information system level 6
  - 2.2.4. Use of artificial intelligence tools 9
  - 2.2.5. Incident management, business continuity, and resilience 10

3. Monitoring, control, and continuous improvement **11**

(The French version prevails)

1. Introduction

1.1. Preamble and objectives

The ABC arbitrage Group (hereinafter, the "Group") develops innovative trading systems and quantitative management strategies across a range of assets, with a focus on niche and short-to-medium-term trading opportunities. It operates in nearly 100 markets worldwide (24/5), providing liquidity through mechanical or systematic signals. Its trading techniques are based on a scientific, data-driven approach to generating alpha, processing billions of data points every day. In this context, the group relies heavily on the quality of its information and technical infrastructure, where data quality and performance are absolutely critical to its operations. This necessitates ensuring a high level of security.

Furthermore, the Group operates within a dense and constantly evolving regulatory framework that places increasing responsibility on companies for data protection and information system security. At the same time, the expectations of the Group's stakeholders are rising, driven by growing demands for transparency, reliability, and resilience throughout the value chain. These requirements cover issues related to intellectual property, licensing, and, more broadly, compliance with digital practices. The Group considers information

security, operational resilience, and business continuity to be essential pillars of its risk management and its responsibility toward its stakeholders.

The group has therefore established a set of reference documents that define security objectives, the measures implemented, general rules and recommendations, implementation conditions, and control mechanisms designed to reduce risks to an acceptable level. The purpose of this document is to formalize, at a deliberately general and non-operational level, the Group's commitments in these areas, without disclosing detailed operational, technical, or organizational procedures, so as not to compromise their effectiveness. The detailed operational, technical, and organizational procedures for implementing security, continuity, and recovery measures are the subject of separate, non-public internal documents that are regularly updated and tested. They help to:

- ensure information security;
- prevent information leaks and safeguard data confidentiality;
- ensure business continuity;
- establish procedures for restoring information systems in the event of a major incident;
- build trust among stakeholders, including service providers and customers.

1.2. Scope

The various principles and rules derived therefrom apply to:

- All entities within the Group;
- The Group's entire information system;
- All of its activities and business lines, regardless of their location;
- All executives and employees of Group companies;
- All third parties who may use the Group's information system and/or host data belonging to the Group;
- All of the Group's information and intellectual assets, regardless of their nature (electronic, printed, handwritten, audio, images, personal data—in accordance with the provisions of the GDPR—data or data flows, etc.).
- All human, technical, and organizational resources enabling the creation, storage, exchange, sharing, and deletion of information between internal stakeholders and/or third parties of the Group, regardless of the medium (hardware components, software, databases or storage and archiving space, equipment related to workstations and client devices, infrastructure and security equipment, procedures and information exchange networks, buildings and premises, etc.)
- All information relating to or belonging to its customers, partners, or any other third parties with whom it has a relationship, particularly information whose alteration or disclosure could harm its reputation or business, or that of its counterparties;
- All information necessary for the management of its personnel, such as identity, salary, or performance evaluation information, the disclosure of which would constitute a violation of privacy.

1.3. Principles & references

The approach is based on an in-depth analysis of the risks associated with the information system, as identified in the Group's comprehensive risk map. It also relies on recognized standards, regulatory requirements, and industry best practices, such as the Information Systems Security Policy (PSSI) guide published by the French National Cybersecurity Agency (ANSSI), the international standards ISO/IEC 27001 and ISO/IEC 27002, and the NIST guidelines.

This framework is part of a cross-functional approach and is consistent with the Group's other internal policies. It is supplemented in particular by the Responsible Procurement Charter, which includes specific requirements regarding security and information protection with respect to suppliers and service providers, as well as by the Internal Regulations, which specify employees' obligations regarding the use of digital tools and information system security, and the penalties applicable in the event of a breach. It is also supplemented by the Personal Data Protection and General Data Protection Regulation (GDPR) Compliance Policy, to ensure that issues related to personal data are systematically addressed.

In accordance with the principle of the weakest link, which holds that overall security effectiveness depends on the most vulnerable component, process, or person in the chain, consistent protective measures are implemented.

2. Safety principles and rules

2.1. Reference documents

System security and integrity have always been a serious concern for ABC arbitrage. Cybersecurity is treated with the same level of importance as other aspects of security. As mentioned in the introduction, the group has adopted:

- an Information Systems Security Policy (ISSP), aimed at ensuring information security (confidentiality, integrity, availability, as well as reliability and traceability), data protection, including personal data, and the management of cyber and technological risks;
- a Business Continuity Plan (BCP), designed to ensure the continuity of critical operations in the event of a major incident that could disrupt their normal functioning (e.g., power outage, communication failure, data corruption or loss, etc.) and to minimize losses;
- a Disaster Recovery Plan (DRP), outlining the procedures for restoring information systems in the event of a major incident affecting technical infrastructure;
- a formalized crisis management process, specifying in particular the governance of the crisis management team, activation and communication procedures, roles and responsibilities, as well as the principles for managing sensitive information and post-incident follow-up;
- an IT Charter, distributed to all employees and appended to the Internal Regulations, which sets forth, in particular, the principles, rules, and responsibilities regarding the use and security of information systems, data protection - including personal data -

and respect for intellectual property. Violations of this policy may result in disciplinary action.

2.2. Key measures implemented

2.2.1. General measures and governance

The Group has clearly defined the responsibilities and roles of the various security stakeholders to ensure that security issues are effectively anticipated, that rules are managed consistently, that they are implemented effectively and in a coordinated manner, and that their enforcement is monitored over time. Governance of the Group's information system security is organized as follows:

- **The Board of Directors** is regularly briefed on key issues related to information system security and operational resilience. It receives dedicated reports covering, in particular, audit findings and the progress of cybersecurity projects. The CTO is available to the Board of Directors to discuss these matters and answer any questions;
- **The Executive Management** bears overall responsibility for information security and ensures that the measures implemented are commensurate with the identified risks. It is responsible for ensuring compliance with commitments, overseeing their implementation, and ensuring that any violations are addressed;
- **The Group CTO** oversees and leads the security strategy. He is a member of the Group Executive Committee;
- **The information systems security team** proposes and plans security initiatives and projects designed to mitigate risks. It plays a coordinating role in the implementation and enforcement of security and cyber-resilience measures. As such, it is involved throughout the entire cycle, covering prevention (awareness-raising, training, etc.), protection, defense, resilience/remediation, and continuous improvement for all of the group's activities;
- **Technical experts** are responsible for the implementation and operation of operational security systems within their scope (maintaining operational readiness, technical monitoring, incident analysis and resolution, etc.), in accordance with defined guidelines. They may contribute to the formulation of requirements and expectations regarding risks;
- **All other employees** play an active role in information security and are required to comply with applicable rules and best practices;
- **Control functions**: Internal control, risk management, and, where applicable, audit functions contribute to the independent assessment of the security framework and its continuous improvement.

This system relies on **clear and appropriate communication channels**, enabling the effective dissemination of information to all internal and external stakeholders involved in security and resilience, both in normal circumstances and during crises, including when digital communication networks are unavailable.

Compliance with security rules is subject to **regular monitoring and checks**. Technical and organizational audits are conducted periodically and on an ad hoc basis to assess the

effectiveness and efficiency of the measures in place and to ensure compliance with obligations and commitments. Applications, databases, and systems are thus verified at various points in their lifecycle, particularly during their integration into the information system, during major upgrades, or on an ad hoc basis if a critical vulnerability is identified. In addition, the Group provides mechanisms for reporting any incident, breach, or situation that could affect the security of information systems.

The policy provides, where necessary, for adapted implementation procedures for security rules, in order to account for specific situations while ensuring an equivalent level of protection. These procedures and specific rules are formalized and formally approved following consultation with the information systems security team, which maintains an up-to-date list of exceptions.

Finally, the group collects and publishes **in its annual report metrics related to cybersecurity, privacy, and data security**, such as the number of reported information security breaches, the percentage of employees who have received awareness training, and the number of tests conducted.

2.2.2. At Human Resources level

The human factor is one of the most common sources of vulnerability in maintaining the security of information systems and is therefore a key focus for the group in this area. The information system's security framework incorporates measures addressing the human factor, combining, on the one hand, initiatives to raise user awareness and foster accountability, and, on the other hand, measures to support and secure usage practices aimed at limiting the risk of human error.

Measures to promote user accountability and awareness include:

- Users are regularly **informed and educated** about their responsibilities regarding information system security to ensure that everyone is aware of the challenges and risks involved. Every employee receives information system security training upon joining the company. This training covers the Group's specific challenges, the key principles of the Information Security Policy, best security practices, and individual responsibilities. The IT policy is provided to each employee upon joining the Group. The documents are freely accessible on the intranet, and reminders are sent to all employees at regular intervals;
- Management and the heads of each operational division are trained in the proper **implementation of the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)**;
- Obligations regarding professional secrecy and confidentiality clauses are included in employees' employment contracts; the IT policy is attached to the internal regulations and includes **penalties and disciplinary measures in the event of non-compliance**;
- All users participate in **mandatory security training and testing** (via a dedicated platform and through internal training) on security principles. Regular awareness campaigns and tests (e.g., phishing) are conducted across the group to assess and strengthen employees' vigilance against cyber threats;

- Users are required (as stipulated in the internal regulations and IT policy) to report and escalate any malfunction, anomaly, suspicious behavior, or potential security incident in accordance with internal procedures and as soon as possible. They must also notify their manager or supervisor of any instance where they are able to access a resource that exceeds their authorized access level. The Group has established a **clear and documented escalation process** for such cases;
- Finally, employees have been trained on the **GDPR**, and procedures have been implemented to ensure that personal data is archived and deleted in accordance with this regulation for all data subjects, including customers and business partners. ABC arbitrage deletes data after a specified period and does not collect personal data from third parties (unless required by law, for example, to ensure a robust anti-money laundering/counter-terrorism financing framework, as described in the policy).

Among the measures designed to support and ensure the safe use of systems, which aim to reduce human risk through procedures and tools:

- The procedure for **managing personnel changes** (new hires, departures, or transfers) includes updating access rights and associated permissions;
- **Functions and access rights** are separated, and two-level validation is in place;
- **End-user devices are protected** in accordance with Zero Trust recommendations, namely: strong, context-based authentication; device posture; network microsegmentation; and encryption of network traffic using Transport Layer Security (TLS) and of data on group-managed drives;
- **Management of user workstation** equipment relies on centralized tools that enable the consistent application of security policies and ensure their ongoing monitoring;
- The group has implemented a **single sign-on (SSO) system** that allows users to access multiple applications and services using a single set of login credentials. This helps reduce the risks associated with compromised credentials and improves overall access security;
- ABC arbitrage also provides each employee with a **corporate password manager**, which is useful when third-party sites do not support single sign-on (SSO).

2.2.3. At the information system level

The security of the Group's information system is based on a set of measures covering asset management, access and identity control, operational security, data protection, threat prevention, and management of third-party risks. These measures are designed to ensure a level of protection that is consistent with and proportionate to the Group's interests.

IT devices management aims to identify, classify, and protect information system resources throughout their lifecycle, taking into account their sensitivity and the associated risks:

- Security and protection issues are taken into account from the very beginning of the procurement process for hardware, software, and digital services. The selected solutions and service providers must ensure a high level of IT security consistent with the risk analysis. The Group therefore applies stringent selection criteria for service providers, which may include preliminary testing of proposed solutions and

robust service level agreements (SLAs). This focus continues throughout the lifecycle of the relevant assets, including during their retirement or decommissioning;

- For critical service providers, the group has backup service providers or solutions in place. These backup service providers or solutions are monitored to ensure that a switchover can be carried out effectively if necessary;
- In the event of an incident, relevant stakeholders, including critical service providers and investors, are appropriately informed about the implementation of business continuity and disaster recovery measures. Management is responsible for coordinating these communications, as well as for implementing any necessary adjustments to information flows or operational processes, in order to ensure consistent and timely information;
- A detailed inventory of information systems, assets, and applications is compiled and regularly updated. Their sensitivity and associated risks are assessed to ensure a clear understanding of threats, vulnerabilities, and potential impacts;
- Assets are protected by appropriate, effective security measures that are proportionate to their level of sensitivity and the identified risks; these measures are regularly assessed and adjusted as necessary;
- An Availability/Integrity/Confidentiality/Evidence (AIC) classification establishes the protection requirements and priorities for the most sensitive assets in order to implement appropriate measures;
- The exposure of sensitive assets to risks of error, improper use, or malicious acts—whether internal or external—is subject to controls, access controls, and prevention and detection mechanisms;
- Measures are in place to ensure the continuity, recovery, and restoration of sensitive assets in the event of a major incident or disaster, within timeframes consistent with operational requirements;
- The setup and configuration of equipment are designed to protect users and minimize risks by strengthening security settings and phasing out obsolete communication protocols or those that serve as vectors for infection, in favor of those recommended by NIST, the NSA, and ANSSI;
- The management of servers, cloud platforms, and networks is automated, enabling rapid, large-scale deployment of configurations and improved tracking of configuration history.

Access and identity controls ensure that only authorized individuals can access systems, data, and infrastructure under controlled and traceable conditions:

- Authorizations and access to assets and information are granted in accordance with the “principle of least privilege” and consistent with user profiles;
- Access and actions performed on information systems or websites are tracked (traceability and accountability) and formally and unambiguously identified through individual accounts;
- Databases and trading platforms use hardware owned by group companies in a secure environment, operating on private systems. No third parties are permitted. Any third-party access to the premises is accompanied by an authorized person, who assumes responsibility for their movements and actions;

- The use of generic accounts is exceptional and must be duly justified, with special attention and specific security measures;
- The list of personnel authorized to access sites, equipment, secure applications, or sensitive data is regularly reviewed.

Operational security aims to ensure the reliable, secure, and controlled operation of information systems, as well as the detection and handling of operational incidents.

- Compliance with best practices is ensured through the formalization of operational procedures accompanied by clear lines of responsibility. Changes are subject to a formalized process, including a risk analysis and validation;
- Resources, IT processes, and the status of the underlying infrastructure are monitored to detect any anomalies or malfunctions so that they can be analyzed and addressed. In the event of an incident or malfunction, alerts are escalated to the teams;
- Obsolete hardware and systems are identified by technical leads, who establish an upgrade or retention plan based on the identified risks.

Data protection relies on measures designed to ensure the confidentiality, integrity, and availability of data, as well as compliance with regulatory requirements, throughout its lifecycle:

- Measures to protect the confidentiality and integrity of data, including sensitive data, are established in advance through specific security protocols and measures, such as - but not limited to - security protocols, data logs, encryption, digital certificates, etc. These services are configured in accordance with best practices recommended by accredited bodies (e.g., ANSSI) and are monitored over time;
- As described in the personal data management policy, the Group ensures the protection, confidentiality, integrity, availability, and security of the Personal Data entrusted to it. It takes all necessary measures to provide clear and transparent information regarding the collection and processing of such data and ensures the implementation of the technical and organizational measures necessary to protect it and ensure that its processing complies with applicable regulations;
- Personal data containing Sensitive Data may be processed in very limited cases and under strict conditions (consent of the individual, data already in the public domain, processing essential for legal proceedings, or explicitly authorized by national legislation).

In addition to the measures described above, **protection against malicious acts** aims to prevent, detect, and mitigate the impact of attacks or behaviors that could compromise the security of information systems:

- All devices are protected by antivirus software, where applicable;
- All remote connections (to remote sites, branch offices, third parties, etc.) are securely authenticated and established using a solution that encrypts data traffic;
- Internet browsing is monitored and logged, and a list of unauthorized websites is maintained and updated regularly. An emergency filtering procedure is activated in the event of the discovery of or an alert regarding data streams or websites identified as malicious;

- Daily scans for internal and external vulnerabilities are conducted, and penetration tests (pen tests) are performed:
    - daily on our externally exposed resources
    - weekly on our internal resources
    - annually by external auditors (different auditors for each iteration).

Relationships with third parties are governed by policies designed to manage risks associated with external access, hosting, or data processing, under security conditions equivalent to internal requirements:

- Whenever collaborating with a third party, risks are assessed, and third parties are granted access only to the environments necessary for the provision of services;
- Contractual safeguards are systematically put in place, covering, for example, liability and confidentiality obligations, data protection, the organizational and technical measures implemented, auditing, reversibility conditions, etc.;
- To ensure the protection of Personal Data and as described in its Personal Data Protection Policy, the Group implements the necessary security measures with any subcontractors, notably through a written contract and a specific confidentiality agreement. It ensures that they provide appropriate technical and organizational safeguards and that they process data in accordance with its requirements and its personal data management policy.

2.2.4. Use of artificial intelligence tools

The use of artificial intelligence (AI) tools in a professional context is strictly limited to uses authorized by the Group and must take place in a **controlled and secure environment.** It must comply with all applicable internal rules, legal obligations, and ethical principles. The Network Administrator reserves the right to implement measures to filter, monitor, restrict, and track usage in order to ensure the security of information systems and compliance with established practices.

Users are required (as stipulated in the internal regulations and IT policy) to ensure the confidentiality of information and, where applicable, **to uphold professional secrecy,** by refraining from entering any sensitive, strategic, or confidential data into an AI tool and by using it in compliance with regulations regarding the protection of personal data, both for data entered in queries and for generated content. Particular attention must also be paid to intellectual property issues and to the fact that content generated by AI remains subject to copyright and applicable intellectual property rules. Users must ensure that the use (reproduction, distribution, modification) of the content does not infringe upon the rights of third parties.

Users are expressly advised that AI systems may produce inaccurate, incomplete, biased, or erroneous results. Consequently, any content generated by AI must undergo **critical, systematic, and thorough human review** before it is used, disseminated, or relied upon for decision-making. Under no circumstances should AI be used as a substitute for users' judgment, expertise, or responsibility.

In general, users should exercise judgment and caution when using AI, comply with applicable laws, and report any issues or concerns. They should participate in training sessions specifically designed for the use of AI.

2.2.5. Incident management, business continuity, and resilience

The Group's resilience framework is based on a structured set of contingency, crisis management, and disaster recovery plans designed to address events that could disrupt normal business operations. Their purpose is to **limit the impact of disruptive events on the Group's operational stability** and to protect its reputation. They establish a framework for governance, decision-making, and communication tailored to exceptional situations, enabling a coordinated and proportionate response.

These measures are part of a comprehensive business continuity strategy and are subject to regular reviews and drills to ensure their relevance and effectiveness over time.

- The Group has implemented a **Business Continuity Plan** (BCP) and a **Disaster Recovery Plan** (DRP), as well as IT Backup and Continuity Plans for all of its business lines. These plans are designed to address all types of scenarios (malicious acts, accidental events, physical security, weather and environmental hazards, intrusion, theft, damage, etc.), including highly unlikely ones. They are based on an analysis of the potential impacts on the Group's operations. They cover alert escalation management, decision-making and operational organization, procedures, communication actions, and the return-to-normal plan;
- Continuity and recovery measures are subject to **regular tests and exercises**, tailored to the relevant activities and conducted at least annually on the most critical environments, in order to verify their operational effectiveness;
- The protection is **tailored to the availability requirements** of the equipment, facilities, and utilities essential to the operation of information systems, as well as to the associated risk. For example, it is designed to meet requirements regarding Maximum Permissible Downtime and Maximum Acceptable Data Loss. The architecture design incorporates service continuity, and all hardware equipment is redundant to prevent any major disruption in the event of a failure and to facilitate the continuity or resumption of critical activities in the event of an incident;
- The organization and resources deployed are designed **to limit the impact of disruptions** that could interfere with or interrupt the normal operation of the IS resources;
- The information system is monitored to detect potential cybersecurity incidents. **Audit events and system and network telemetry are centralized**, and alerts are triggered when thresholds are exceeded or a failure occurs. Critical logs are protected. In addition to automatic alert mechanisms, users are required to report any security anomalies;
- **Indicators** are used to identify and characterize information security and cybersecurity breaches (origin, impact, etc.);
- All hardware equipment is covered by **maintenance contracts**, the vast majority of which provide for 24-hour support with a guaranteed response or replacement time;

- A **process for handling infections and applying security patches** has been established for all components of the information system and is known to the technical contacts. Emergency procedures are in place in the event of a critical alert. Infection incidents are monitored and subject to reporting and analysis;
- In the event of a failure or incident, a **crisis management team** is activated in accordance with established governance procedures to assess the situation and coordinate the decisions and actions to be taken. The analysis of security incidents leads to an action plan (preventive and corrective measures) designed to improve existing measures or create new ones.
- In the event of an incident, **appropriate controls and verifications** are performed to ensure data integrity and consistency prior to the full restoration of system operations, including for reconstructed data.

3. Monitoring, control, and continuous improvement

The Group is committed to a **process of continuous improvement** in these areas: regular internal and/or external audits and assessments are conducted to evaluate the overall effectiveness of the system and identify areas for improvement. The Group's security framework and policies are reviewed and updated at least once a year or whenever a relevant event occurs, and at a minimum in the event of changes in business operations, significant organizational changes, or changes in the technical or regulatory environment, as well as based on lessons learned from incident handling.

The Group regularly assesses the effectiveness of its digital security and operational resilience strategy. To this end, the technical team ensures that technologies and practices remain state-of-the-art, while actively monitoring new threats and vulnerabilities.

An anonymous reporting system has been established to allow employees and third parties to report any suspected misconduct without fear of retaliation. Anyone who deems it necessary may submit a report via email to lanceurdalerteabc@gmail.com or by mail to 18, rue du 4 septembre, 75002 Paris. Confirmation of receipt of the report, along with a reasonable and foreseeable timeframe for reviewing its admissibility and details regarding the follow-up actions taken, will be provided as soon as possible. In the case of an anonymous letter, no confirmation of receipt or information regarding the follow-up actions taken may be provided to the sender. Reports are processed according to a formalized procedure, ensuring their analysis, follow-up, and the implementation of appropriate corrective or disciplinary measures in the event of a proven violation. All details are available in the dedicated public procedure.