360X AG

Information Risk Management Policy

Version: 0.1

Document properties

Version	Comments
Responsibility	Information Security Officer (ISO)
Validity period	Unlimited
Review Interval	Annual
Next Review	*TBD*
Filename	Information Risk Management Policy

Document status and approval

Status	Version	Date	Name of Department/ company
Created	0.1		

Table of Content

List of Tables

List of Abbreviations

Abbreviation	Meaning
360X	360X AG
3LoD	Three-Lines-of-Defense
AktG	German Corporation Act
BAIT	Supervisory Requirements for IT in Financial Institutions
BDSG	Federal Data Protection Act
BSI	Federal Cyber Security Authority
ESMA	European Securities and Markets Authority
GDPR	General Data Protection Regulation
ICS	Internal Control System
IRM	Information Risk Management
ISM	Information Security Management
ISO	Information Security Officer
MaRisk	Minimum Requirements for Risk Management
SoD	Segregation of Duties
SSH	Secure Shell
VPC	Virtual Private Cloud
VPN	Virtual Privat Network

1. Introduction

1.1. Purpose

We, as 360X AG (“**360X**” or “**the Company**”) offer financial instruments on a digital trading platform, which is used to broker them between users of the platform.

To make this possible, we apply a variety of process steps. These include e.g. the collection of a comprehensive list of information on the assets from their owners, the listing and delisting of instruments on the 360X platform and finally the brokerage of those instruments between investors and assets owner, together “users” (also see the process landscape for an exhaustive list). Through all our processes, we adhere to the highest quality, security, and compliance standards in the industry to provide the best experience for our customers.

We position ourselves as a secondary marketplace for financial instruments of alternative asset classes, such as art and real estate, and offer our services through online channels. We must ensure confidentiality, integrity, availability, and authenticity of 360X’s information and its supporting processes, systems, and networks.

This guideline forms the overarching framework for the Company's Information Risk Management (“**IRM**”). This document was prepared in coordination with the general IT strategy framework. The objective of the IRM Guideline is to implement the components of an Information Risk Management System with the participation of all relevant offices and functions in a competent manner and free of conflicts of interest.

In order to do that, this policy is based on the regulations DIN EN ISO/IEC 27001:2017, the IT-Grundschutz Compendium of the Federal Cyber Security Authority (“**BSI**”), the General Data Protection Regulation (“**GDPR**”), Federal Data Protection Act (“**BDSG**”) as well as the Minimum Requirements for Risk Management (“**MaRisk**”) and the Supervisory Requirements for IT in Financial Institutions (“**BAIT**”). Furthermore, all requirements resulting from the European Securities and Markets Authority (“**ESMA**”) Guideline on Outsourcing to Cloud Service Providers (ESMA50-164-4285) have been considered.

1.2. Background

According to BAIT the IRM specifies requirements for processing and sharing of information in business and service processes. These shall be supported by data processing IT systems and related IT processes. Therefore, the scope and quality shall be based on the Company’s internal operating needs, business activities and risk situation (see AT 7.2 sect. 1 MaRisk). The IT systems, the related IT processes and the other components of the information domain shall ensure the integrity, availability, authenticity, and confidentiality of data (see AT 7.2 sect. 2 of MaRisk).

In summary, BAIT defines that the Company shall define and coordinate the tasks, competencies, responsibilities, controls, and reporting channels required for the management of information risk (see AT 4.3.1 sect. 2 of MaRisk). To this end, the Company shall set up appropriate monitoring and steering processes (see AT 7.2 no. 4 of MaRisk) and define the related reporting requirements (see BT 3.2 sect. 1 of MaRisk).

1.3. Scope of Application

The Information Security Officer ("**ISO**") of the Company hereby adopts the present Information Risk Management Policy as part of the company-wide information security management ("**ISM**"). The scope of application is 360X. Insofar as the Company concludes contracts with third parties whose subject matter falls within the scope of the policy, it will oblige the contractual partner to comply with the policy.

This policy is subject to at least an annual review. In case of major organizational changes, such as changes to company or IT strategy, adjustment of organization, or changes to the overall risk situation of the company, ad-hoc reviews must be carried out.

2. Targets of Information Risk Management

IRM adapts the generic process of risk management and applies it to the integrity, availability, and confidentiality of information assets and the information environment.

The targets of the IRM are derived from the business strategy, correspond with the IT-strategy and can be shown as follows:

- Support the ISM to achieve their goals
  - especially for integrity, confidentiality, and availability (see chapter 5.3 and 6).
- Protecting the Company, its staff, and its customers from information risks where the likelihood of occurrence and the consequences are significant (see chapter 6).
- Provide a consistent risk management framework in which information risks will be identified, considered, and addressed (see chapter 6).
- Ensuring that the IT systems used to process and share data are adequate to meet
  - the applicant's business needs,
  - operational requirements and

To ensure these targets the IRM aims it treating identified information risks adequately and thereby effectively protect information.

For this purpose, possible deviations from the information security requirements and information risks are controlled. These are checked for plausibility regarding the respective assessment of the affected department and the defined measures. In addition, the appropriate assessment, the defined measures as well as the deadlines and responsibilities set for each information risk are checked at least once a year.

3. Statement of Risk Appetite

This policy should be read in conjunction with the Company's Risk Management Policy which identifies the overall as well as risk specific risk appetite of 360X.

The risk appetite for the identified risks of the Company is derived from the risk strategy which is derived from the Company's business strategy.

Outsourcing Risk

In the context of information risk management these are information security risks that arise from the engagement with third parties due to performance issues of services and/or infringement of contractual obligations. This includes especially the risk of poor confidentiality and security but also the risk that legal requirements, specifically regulatory requirements for outsourcings are not met.

The Company's business model involves the delegation of certain functions to external third parties. The Company has no tolerance for the actions of third party providers, which threatens the availability, integrity, confidentiality and authenticity of 360X data assets, e.g. due to inappropriately executing business activities of the outsourced partners. Therefore, the Company aims to secure satisfactory service from the third party providers, whilst limiting and mitigating risks (see 6.1.2, 6.5 and 6.8) for the respective services.

Operational Risk

These risks are information security risks of economic loss or other adverse impact resulting from inadequate or failed information security, as well as from the occurrence of external events which interrupt the execution of normal business activities.

By providing a digital technical platform there are operational risks such as theft (cyber-attack), incorrectly valued positions, system failures, general process weaknesses or failure of control mechanisms, particularly regarding IT.

The Company aims to minimize losses on information security and business continuity incidents such that they do not impact the Company in a negative manner. The Company aims to ensure that employees are adequately informed to ensure the protection of information and that measures are taken to minimize business disruption.

Compliance Risk

These risks are information security risks that arise from the failure to act in accordance with personal data protection laws. These include for example the infringement of the GDPR, or similar regulations as well as non-compliance with internal guidelines for data protection.

By providing a digital technical platform there are compliance risks such as fraud or insider trading.

The Company aims to minimize losses on data protection incidents, e.g., breaches (see Data Protection Policy), in a way that they do not impact the Company in a negative manner. 360X aims to fulfil all internal and external data protection obligations in a way that all requirements and responsibilities concerning data are met, e.g., protection data from unauthorized third parties and handling data correctly.

4. Organization of Information Security

The IT-security organization of 360X is described in the Information Security Policy as well as its subordinate policies. These also includes the risk management.

For further information see Information Security Policy.

5. Roles and Responsibilities

The Head of IT is responsible for IT at 360X and leads the Engineering & IT division, which includes the Security, IT Development and IT Operations units. However, the Head of IT has the main responsibility for IT Security at 360X and the IT Security Team is responsible to ensure that all the necessary activities and controls are in place to comply with this security policy. These activities include, but are not limited to, processes regarding the IRM e.g., the determination and safeguarding of the protection needs.

The Company maintains adequate qualitative and quantitative staffing levels in the Company's IT to ensure smooth business operations. IT staffing requirements are reviewed on a regular basis. The planning of staffing considers future expense drivers such as forecast business development, new legal and regulatory requirements, and changes in customer needs or the threat situation.

The contact for all questions regarding this policy and owner of this policy is the ISO.

In general, the following responsibilities regarding IRM are defined:

5.1. Management Board

The Management Board is the supreme decision-making body. It adopts this Information Risk Management Policy at the proposal of the ISO.

The Management Board has ultimate responsibility for the management of risk and the establishment of proper controls as part of its continuing drive to enhance corporate governance in 360X.

For further Information see Information Security Policy.

5.2. Information Security Officer

The ISO is responsible for controlling possible deviations from information security requirements and information risks. The ISO checks the plausibility of risks regarding the respective assessment of the affected department and the defined measures. In addition, the ISO checks at least once a year the appropriate assessment, the defined measures as well as the deadlines and responsibilities set for each information risk.

In addition, the ISO coordinates and monitors the processes described within the organizational policies.

The contact for all questions regarding this policy and owner of this policy is the ISO.

For further Information see Information Security Policy.

5.3. Other functions

The role other functions encompass all persons employed at 360X. Everyone has a role in the effective management of information risk. All employees will actively participate in identifying potential information risks in their areas and contribute to the implementation of appropriate mitigating actions. Employees are responsible for compliance with the specifications defined in separate policies. They are required to pay attention and vigilance in handling the information technology provided. The employee undertakes to handle the information entrusted to him in a proper, security-conscious, and purpose-oriented manner. Employees should always be aware of the importance of IRM and actively participate in preventing and combating material and non-material damage. Employees should handle the information systems and the data stored and processed on them responsibly and ensure that company and business interna are protected. The protection of the integrity, availability and confidentiality of assets is part of the responsibility of the owners of the respective assets. In the event of irregularities, employees must immediately inform the ISO and their supervisors.

6. Information Security Risk Management

The Company's IRM ensures that the IT systems used to process and share data are adequate to meet the business needs, operational requirements, and risk management requirements of 360X.

6.1. Risk Overview

Maintaining a risk register is essential to oversee and control potential und existing risks. 360X's risk register acts as a repository for all risks identified and includes additional information about each risk (e.g., nature of the risk, reference and owner, mitigation measures) The risk register contains all potential and identified information security and operational risks.

For more information see Risk Management Policy.

6.1.1. Business Environment

As a highly digitalized financial service provider, we operate in a dynamic environment subject to a constant change. The development of the relevant market is characterized by uncertainties. There is a high degree of dependence on the market for financial instruments and the underlying assets itself. Due to the function as an investment broker for financial instruments, as well as through participations in the verticals, there is a dependency on the price and market developments of the financial instruments. As a specialized service provider in the environment of financial instruments, this concentration of risk is consciously entered into. Thus, there is a risk of having to adjust the business model in order to remain competitive.

Cyber security aspects are becoming increasingly important in this business environment. Cyber risk is a significant risk and can come in many forms including distributed denial-of-service ("**DDoS**") attacks and phishing attacks. In addition to the risk of regular cyber-attacks in this business environment, the regulatory requirements are still very much in development, which is why the risk of changes in regulatory requirements is a constant companion for us.

Name	Probability	Impact	Mitigation

Unforeseen Market Changes	Low	Medium	Decisive monitoring of developments and trends in the relevant markets in order to react to possible changes in competition and users at an early stage to stay competitive. This includes for e.g., the adjustment of the pricing, target group or design of our services or the accepting of new or the sorting out existing cryptocurrencies for trading via the platform.
Cyber-Risk	Medium	High	Employment of firewalls, antivirus, anti-malicious and anti-trojan software, thus providing security to their systems and reducing the chances of such attacks being successful.

Table 1: Potential information risks arising from business environment

6.1.2. Business Model

As mentioned in the introduction the business model of the 360X is based on the provision of a digital brokerage platform, allowing users to find other users to trade (purchase or sell) financial instruments. Investors and asset owners are introduced to each other via the platform 360X provides.

360X works in close collaboration with so-called “verticals” and “non-verticals”. These provide independent implementation support on value growth strategies for the underlying assets of the asset owners. If the asset owner decides to onboard her asset at the 360X platform, the vertical will support, if needed, the administrative activities (e.g., formulation of the instrument terms) required for listing and approval.

There is a risk due to the dependence on other players, especially the Solaris Bank AG and Solaris Digital Assets GmbH. If, in the event of the failure of the players, adequate replacements for the failed service provider cannot be found or cannot be found in time, no further trading via the platform would be possible either. The Solaris Bank AG and Solaris Digital Assets GmbH are responsible for the settlement of the transactions mediated via the platform.

Name	Probability	Impact	Mitigation
Third Party Dependency Risk	Medium	High	Where possible redundancies are in place to ensure that the business continuity will not be affected.
Data Access through Third Party	Low	High	Due diligence procedures and measures are in place as well as reviews, assesses and background checks. We obtain company documents, certifications, references and ensure that the third party is adequate, appropriate, and effective for the task we are employing them for. Additionally, processes are in place for reviewing the ongoing suitability of the third parties, such as audit arrangements.

Table 2: Potential information risks arising from business model

6.1.3. Operational Information Risk

Operational risk is defined as the risk of loss which results from inadequate or failed internal processes, procedures, people and systems or from external events.

360X is highly reliant on IT systems and is using computer hardware and software equipment in order to carry on its activities. Human, technical or procedural errors could lead to a failure or restriction of the IT or infrastructure. In this case, it would no longer be possible for users to buy or sell financial instruments authorized on the platform. There is no direct possibility to switch to other platforms. The target is to minimize service disruptions of any form.

Risks associated with fraud and embezzlement, due to insufficient segregation of duties and due to a lack of effectiveness of oversight controls and processes, are present in all institutions. Periods of substantial increase in trading volume or number of clients as well as the introduction of new products or instruments, introduce risks originating from the inability to perform existing controls and procedures. Such risks may lead to financial losses, service disruptions and can even 360X's reputation. Hence, the objective is to decrease the likelihood of the aforementioned impacts.

To a certain extent, 360X relies on manual inputs and manual monitoring tools, which lead to the risk of human error, miscommunication, and timely oversight. Additionally, a lack of sufficient reconciliation to external sources may be caused by a lack of automation. The aim is to minimize the need for manual activities, thus eliminating the risk of human error which may cause financial losses, service disruptions and could even affect 360X's reputation.

360X is exposed to the risk of internal system failure, in the form of algorithmic and IT systems malfunctions resulting in the unavailability of data and the discontinuation of service.

Additionally, we are aware that there are always several potential risks through the operation business in regards of information security. This includes for instance that:

- Data gets manipulated by third parties
- Data gets extracted by third parties while being submitted
- Data gets lost through the submission
- Third parties try to get access to data assets

These risks are always present, especially for the following processes:

- Tokenization of assets
- Approval and listing of instruments on the Platform
- Revocation of listed instruments from the Platform
- User onboarding process
- Purchase & sales processes
- Completion of instrument measures
- User offboarding from the Platform

Name	Probability	Impact	Mitigation
Business Continuity Risk	Low	High	Business Continuity plan
Control Failure	Low	High	Segregation of Duties ("**SoD**"); Internal Control System ("**ICS**"); Three-Lines-of-Defense ("**3LoD**")
Manual Activity Risk	Low	Medium	Continuously investing in automated processes; continuous improvement in Risk Controlling
Fraud	Low	Medium	Automatic system screening for fraud characteristics as well as manual reviews of all suspected transactions; 3LoD
Internal System Failure	Low	Medium	Hardware and software backup systems are in place (i.e. backup servers that provide normal operations to their system.)
Data Manipulation	Low	High	Use of secure information channels for data transmission like Virtual Private Networks ("**VPN**") Management Framework. Several controls and principles like least-privilege, Segregation of Duties, Four-eyes controls, recording of activities. Access to all systems and servers shall require the use of cryptographic methods (encryption, digital signatures, multi-factor authentication) for authentication.
Unauthorised data extraction	Low	Medium	Use of secure information channels for data transmission like VPNs. Access Management Framework. Several controls and principles like least-privilege, Segregation of Duties, Four-eyes controls, recording of activities. Authentication credentials are always be encrypted in transit. Access to all systems and servers shall require the use of cryptographic methods (encryption, digital signatures, multi-factor authentication) for authentication.
Data loss	Low	Low	Using Virtual Private Cloud ("**VPC**"), Backups, use of secure information channels for data transmission.
Unauthorised access	Low	Medium	Access Management Framework. Several controls and principles like least-privilege, Segregation of Duties, Four-eyes controls, recording of activities. Authentication credentials are always be encrypted in transit. Access to all systems and servers shall require the use of cryptographic methods (encryption, digital signatures, multi-factor authentication) for authentication.

Table 3: Potential operational information risks

6.2. Information Network

The information network is regularly inventoried including business relevant information, business processes, IT-systems as well as network- and building infrastructure. A current overview over the components of the set information network as well as its dependencies and interfaces can be viewed here: [Insert here reference to an architecture overview]

6.3. Protection requirements analysis

All relevant positions including the specialized departments are involved within the protection requirements analysis. The involved units are free of conflict of interest. This is ensured with the Conflict-of-Interest Policy. There is an inventory of the information network on which the protection requirement analysis is built upon.

The determination of the protection needs is based on the following criteria:

- Availability
- Integrity
- Confidentiality
- Authenticity

It shows the consistency of the resulting protection needs comprehensibly and can be found here: [Insert here reference to Protection needs assessment]

6.4. Preparation of Risk Analysis

Prior to the actual risk analysis, the Company performs the following preparatory work:

6.4.1 Definition of Information Risks

Information risks are risks that relate to the loss of integrity, confidentiality, availability or authenticity of information and can be in physical, digital or spoken form. This also includes risks arising in outsourced business processes and services.

IT risks are digital information risks that generally arise from the IT environment and can, for example, affect IT management, IT control, the internal control system of the IT organization, IT strategy, IT policies, or the use of information technology in general.

Non-IT risks relate to non-digitized information, such as paper or voice.

Cyber risks are risks that threaten the security of 360X information from outside via interfaces.

6.4.2 Definition of IRM Process

With a view to overarching risk management measures, the Company has opted for uniform treatment of all operational risks, which also include information security risks. The identified information security/IT risks flow into the operational risk process and are integrated into 360X’s risk management framework.

6.5. Risk Analysis

The Company understands risk analysis, analogous to the ISO standard 27005, to be the complete process for assessing (identification, evaluation and assessment) and dealing with information risks.

For this purpose, the ISO of 360X creates a guideline (see Risk Management Policy) that defines the basic requirements for performing an information risk analysis. To conduct an information risk assessment process to determine how risks will be measured the establishment of appropriate risk criteria is needed. Therefore, various risk acceptance criteria are defined according to risk appetite and based on the risk strategy of 360X.

If necessary, but at least annually, the entire risk inventory of all relevant information risks is updated. Information security risks are classified at 360X according to information risk class and probability of occurrence. Depending on the assessment, information security risks are assigned to the risk categories "low", "medium", "high" and "very high" according to 360X's risk matrix.

Category	Characteristics
Very High	• The likelihood of the threat affecting the business is very high, as this threat is critical to this business, or has direct relevance to the business functions, or there is significant historical and industry evidence of exploit and threat. • Confidentiality and integrity of information must be guaranteed at all times. • The failure of information systems could lead to total collapse of the company or have severe consequences for the Government, its clients, partners and the public. • Information is most likely classified as “Highly Protected”.
High	• The likelihood of the threat affecting the business is high, or has direct relevance to the business functions, or there is significant historical and industry evidence of exploit and threat. • Information must be correct and any errors detectable and avoidable. • Short periods of down time can occur, but processes must be carried out within a strict timeframe. • In the event of system damage, critical areas can no longer function resulting in a considerable harm to the company, the Government, its clients and the public. Information is most likely classified as “Protected”.
Moderate	• The likelihood of the threat affecting the business is medium, as this threat may be relevant to this business, or has some relevance to the business functions, or there is some historical and industry evidence of exploit and threat. • Confidentiality of information must be guaranteed for internal use only. • Minor errors in data can be tolerated and business activities will allow moderate periods of downtime.
Low	• The likelihood of the threat affecting the business is low, as this threat is not relevant to this business, or is not relevant to the business functions, or has a historically low track record of exploit or vulnerability. • Confidentiality of information is not required. • Errors in data and downtime of systems will have minor impact to the company. • The consequence of damage is only a minor disruption to the company, the Government and its clients, with limited impact on the public.

Table 4: Risk categories

6.5.1 Risk Identification

In the risk inventory process 360X identifies and records all risk exposures (including information risks) that arise from its business activities. The risk inventory process takes place at least annually as well as on an ad hoc basis, if required. In particular, adjustments to the previous inventory might be necessary by introducing new financial instruments. The risks identified with the financial instrument are included in the risk register. Additionally, the risk inventory process is performed on an ad hoc basis, e.g., in the event of a change in materiality for the business model or as a result of significant external influences on the business model.

Interviews besides historical analysis on previous events and audits on a regular basis, conducted by 360X's Risk Controlling function are one of the most effective methodologies to identify risks. The method enables the incorporation of the expertise of each employee in the risk identification process, thus identifying risks which could not be identified by an outsider. Two types of interviews are conducted: The first one has no structure and aims to allow employees to share their concerns regarding their departments. The second stage is a structured interview. The target is to go through the procedures in place at the time and to brainstorm with the experts of each department on potential risks. The combination of the two types of interviews allows for a more comprehensive approach.

360X's will keep a risk register as a foundation for evaluating existing and potential risks. Risks identified through interviews or materialized risks are recorded in the risk register. For more information see Risk Management Policy.

6.5.2 Risk Measurement

The Risk Controlling function, together with the risk owners, have the responsibility to assess whether an identified risk is material (classified as “high” or “very high”). Materiality is usually assigned based on a high-level qualitative assessment of the respective risk. Risks that appear material are being considered more carefully to measure their impact precisely using qualitative and quantitative techniques as well as stress testing. For more information on qualitative assessment, quantitative assessment and stress testing see Risk Management Policy.

6.5.3 Risk Treatment

For information security risks that are not accepted (or should information security risks not exhibit the targeted risk level), measures are defined, implemented and documented. These measures can have different objectives:

- Risk avoidance,
- risk reduction, or
- risk transfer.

Risk acceptance can only be decided in exceptional cases for information security risks in the "medium", "high" and "very high" categories.

For risks categorized as "very high", specific measures are adopted to adequately address these risks.

In addition, appropriate controls (see 6.8) are defined in 360X to ensure the completeness, accuracy and timeliness of all information security risks.

6.6. Reporting

The ISO will report to management on the status of IRM on an as-needed basis, but at least quarterly.

This means that in the last calendar week of each quarter, the ISO regularly prepares a quarterly report on the status of IRM related processes that has been conducted since the reporting date of the last quarterly report and submits it to the management board of the Company. The quarterly report shall contain at least the following:

- Status of the information risk situation of 360X.
- Results of the protection needs analysis.
- Results of the risk analysis.

Reports on an as-needed basis means that the ISO immediately informs the management board of the Company of any serious deficiencies.

6.7. Risk Monitoring and Re-Performance

Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of 360X and include regular management and supervisory activities.

Regarding risks, which cannot showcase the aspired risk level, the respective measures must be defined and documented. Their implementation must be planed and will be executed with the aid of an appropriate project management. The catalogue of measures created shows, which security requirements are defined for the individual protection needs categories. The catalogue is monitored ongoing.

6.8. Risk Mitigation

360X has established a risk based controlling environment, which is suitable for the prevention, identification and defense of risks. It follows a holistic approach and covers the entire company. It additionally serves to appropriately monitor and manage the risks. The risk managing and controlling processes as well as the methods and procedures for risk qualification are regularly, as well as in cases of changing conditions, reviewed and where appropriate adapted. A current overview of controls can be viewed here: [Insert here reference to an overview]

6.8.1 Access Controls

To protect the data and users of the company, we have ensured several access controls. For further information see Access Management Policy.

Physical access:

The company considers physical security measures to be another key component of the overarching security of information. Physical access methods, procedures and controls are in place to prevent unauthorized access to data, assets and restricted areas. Physical access to the company's offices is only allowed to authorized people with personal electronic identification cards. These access cards are issued to the Company's staff by the person responsible for the respective office. The authority to issue the cards and grant access is limited to the office manager and authorized representatives. Visitors to the Company's office must register and will be escorted when entering the premises.

Remote access:

Remote access to both the company workspace and production environment servers are protected by tools and controls provided by the GCP being used and configured by the Company.

Authorized access to the GCP hosting environment is directly from the corporate office or via VPN to the applicant's office and then to GCP using SAML and two-factor authentication.

The Company's employees are given remote access to the internal production network environment only on a least privilege basis. Traffic entering the company's production network is monitored and controlled by a firewall and monitoring tools implemented by GCP and configured by the company.

Remote users are automatically disconnected from production servers after a predefined period of inactivity and must log in again to reconnect to the network.

In addition, access to production systems is restricted to selected staff and these systems require additional layers of security and authentication.

Monitoring and security practices are continuously updated as new potential threat/risk assessments require.

Access to all systems and servers shall require the use of cryptographic methods (encryption, digital signatures, multi-factor authentication) for authentication. No system shall allow access solely through a username and password.

Production environment logical access:

The production environment is separated into VPC which are assigned to customers. Access to the customer environment web application interface is performed using personal production username and password for relevant users. Admin access to the production servers is performed using a VPN between 360X' offices and the Data Centers, which is uniquely identified. This access still requires a specific production username and password, which is available to each relevant user. Developers do not have access to the production environment. The access to the production servers is performed by using Secure Shell ("**SSH**") keys and is restricted only to authorized personnel. The components are logged and monitored for errors and performance issues are recorded on an internal monitoring infrastructure. Errors are reported into an automated internal communication channel.

The access to the datacenter management interfaces is restricted only to authorized personnel. In addition, access to the production environment and databases and other production-related environments, is granted by the appropriate personnel, based on the employee role and documented within a dedicated tool. The access to the backup and offline storage is restricted only to authorized individuals. Staff is provided with the minimal access rights required to carry out their duties. New users accessing 360X system are granted access upon notification from the HR department. A detailed ticket is opened in the IT Management ticketing system using a new hire template. This template includes all user detailed permissions. Additionally, strong password configuration settings, where applicable, are enabled on the domain, application and database.

7. Outsourcing

When services are outsourced an agreement will be made regarding the risk management. The compliance with it will be monitored and regularly tested.

For further information see Outsourcing Policy.

8. Awareness and Training

Organizations must conduct awareness and training on information security for staff of the organization to ensure awareness of staff for the importance of information security. Regular training ensures that staff remain aware of their responsibilities follow necessary guidelines to maintain compliance requirements. This ensures the protection of personal data and the prevention of personal data breaches.

Therefor our goal is that all staff understands the IRM and associated laws requirements, has ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for their role.

9. Other measures

This policy is reviewed and updated when needed, but at least annually, by the policy owner, following consultation with the IT Policies, Procedures, Security and Standards Working Group.

In addition, to ensure appropriate behavior and conduct we have developed a Code of Conduct, which contains a collection of internal guidelines and regulations for our employees on how to act in their daily work (also see Code of Conduct).

10. Violations and Sanctions

Intentional or grossly negligent acts that violate safety rules can result in financial losses, harm staff, business partners and customers, or jeopardize the company's reputation. Deliberate violations of mandatory safety rules can have consequences under labor law and, under certain circumstances, also under criminal law, and can lead to recourse claims.

Any significant violation(s) of this policy will be documented and brought to the attention of management as well as the ISO. Material violations shall be dealt with in an appropriate manner and may lead to disciplinary action, up to and including termination of employment. Non-staff members, including consultants, may be subject to termination of contractual agreements, denial of access and/or both criminal and civil penalties.

11. Entry into force

This policy has been released by the management of 360X and will come into force on XX.XX.20XX.

Released by: Management Board

[Place, Date, Sign of Management]

12. Document History

Version	Date	Amended by	Amendments / Comments
0.1	2022/XX/XX		