Information Security Policy

Summary

Table of contents

1 Introduction

Most of the company activities are dependent on information managed within the organization and related business processes. The core business processes are and all kind of data flows are executed with the help of information systems functionalities. The information system importance increases their exposure to variety of threats. The company information assets are vulnerable to variety of physical, logical and natural threats. Information security purpose is to protect the critical assets and business processes of the company ensuring the long-term operation and the safety of all interests of customers, employees and partners and compliance with legal and regulatory requirements such as GDPR.

Since there is no fully reliable information system, ZigZag Global Ltd and its entities takes proactive measures and also reacts promptly to any information security incident. The corrective actions consist of recovering of lost or manipulated data and restoring the information system operating state. Information security processes established at ZigZag Global Ltd consider also local legal and regulatory requirements for protection of information assets.

General objectives of the information security in ZigZag Global Ltd and its entities are covered by:

- Protecting of information security **confidentiality** that ensures only authorized access to the information assets of the company.
- Preserving data **integrity** consists of security mechanisms that avoid intentional or accidental information disruption, change or/and manipulation.
- Assuring data **availability** guarantees of digital and printed information availability and flawless systems operations.
- Ensuring information **non-repudiation** avoids information litigation through strong user authentication and the enforcement of electronic signatures, digital certificates and implementation of strong authentication and authorization methods.
- Providing **traceability/proof** of a technical event (e.g. technical security traces or logs) or of a business-related action (e.g. audit trail) and verifying that trace, must be associated with a person and reference for the time being performed.

2 Coverage

This document is made for the use of anyone dealing with the technical, procedural or information resources of ZigZag Global Ltd. The defined in the Policy principles are valid for all digital, analogues, verbal or hard copy (paper-based) exchanged or stored data. The company Information Security Policy is addressed to all workforces with no exceptions.

Internal employees – This policy is valid for all company employees, trainees, IT department staff members, subsidiaries of ZigZag Global and other company members operating within the ZigZag Global internal network, with no exceptions.

External contractors – Compliance with the Policy must be ensured within the legal contract, signed with external for the company workforces:

- Service providers and external representatives dealing with company information
- Partners and third parties that process information on behalf of ZigZag Global
- Independent external audit teams

3 Information security design, implementation, monitoring and review

The Information Security team designs and assists during the implementation of an Information Security Strategy which includes:

- Define appropriate information security action plan for ZigZag Global
- Implementation:
    - Normative framework
    - Information security awareness
    - Information security risk assessment
    - Security measures and controls
    - Integration of the Information security requirements to related business processes
    - Permanent supervision and independent audit checks
- Monitoring:
    - Updated information systems security procedures and related processes
    - Regularly performs independent information system audits
    - Analyzes the incident reports and change records
- Maintenance:
    - Corrective actions upon reviews
    - Communication of new parts within the established security controls
- Review:
    - The Information Security Policy shall be reviewed at least annually

- Updated as needed to reflect changes to business objectives or the risk environment

4 Policy principles

4.1 Risk assessment and management

4.2 Vulnerability Management

The objective of the information security risk management is to identify, quantify and manage information security related risks, their probability and potential impact on the business strategy of the company. Information security risk assessment is a continuous process which must be considered during the implementation of new business process and/or changes of already existing company processes, against latest internal and external threats.

Responsibilities for the information security risk management under the overall company risk management are clearly assigned across the company and adequately communicated to the corporate workforces.

ZigZag Global shall carry out an annual risk assessment process that would identify major strategic developments in the industry, emerging threats, & vulnerabilities, to business and IT assets of the company and report results in a formal risk assessment document.

4.3 Management of company information assets

The ZigZag Global assets include information, software and physical assets. Information assets are all assets which contain any data. Information assets inventory is managed and updated within the company in terms of evaluation of current and/or new data types. The technology assets of the company are used by the employees only for work purposes and with respect to the information security principles.

4.4 Data classification

In order to provide reliable security information management, ZigZag Global has accepted security classification that concerns company data, devices and network connections. Based on their credentials, Users receive Security classification clearance in order to have access to data and the network infrastructure. The company security levels are presented in a separate policy – Data Classification Policy.

4.5 Personnel security

ZigZag Global employees are considered the most important corporate asset, requiring constant assistance and management with respect to the Information Security. Personnel security consists of minimum measures to be taken so that the

company employees and other workforces (entities, service providers, contractors, trainees and third-party users) are being protected and informed for their information security related responsibilities.

Newly hired employees of the company must be informed and undertake in written to comply with the internal, legal and regulatory requirements for Information Security.

4.5.1 Information Systems Security Awareness Program

Compliance with information security rules is essential to the business strategy of ZigZag Global. Every employee has the responsibility to become acquainted with the information systems security principles and respect them during execution of their daily duties. In cases of miss compliance with ZigZag Global internal information security principles, which might bring risks for the company, disciplinary sanctions are enforced by Human Resources Department. ZigZag Global member users and external service providers receive the appropriate for their business line awareness training, related to the latest updates of security requirements, control measures and vulnerabilities, which might appear on the company information systems.

4.5.2 Confidentiality Agreement

Confidentiality and non-disclosure agreements inform users that the information is confidential and subject of rules to which must be respected. Contractors, vendors and consultants which services are directly or indirectly related to access to data of the company, either in electronic or hard copy form, sign confidentiality agreements for every single assignment and before being granted with access to corporate information. The External Company must send to the Information Security team copies of the declarations signed by external employees involved in the execution of the services. That is the way the staff from another company officially to confirm that they are aware and accept to respect ZigZag Global Information Security principles. Only after the non-disclosure agreement is signed, the access to the company technical environment and/or sensitive data is provided. Same applies in case internal data must be provided to vendor in order to participate in tenders and/or for offer preparation.

4.5.3 Electronic Communication Management

In order to reduce the risks associated with electronic communication, the internal ZigZag Global rules for digital data exchange are valid for all employees and external workforces with authorized access to the company technology environment.

4.6 Infrastructure security

Information system components must contain integrated functionalities necessary for protected and reliable operational services. They must be exploited in compliance with the company information systems security principles, legal and regulatory requirements. The security related composite parts must be designed, equipped,

configured, integrated and maintained so that they do not expose on vulnerabilities corporate information systems and reduce risk impacts to the acceptable minimum for any business units from ZigZag Global.

4.6.1 Logical Access Control

Logical access controls for systems, applications and data are designed to prevent risks related to unauthorized access to sensitive data and incorporate the necessary balance between business needs and preventive actions. The published Access Control Policy is applicable for all information assets and technical resources designed, implemented, maintained and operated within ZigZag Global information technology environment.

4.6.2 Protection of Information Flows

The protection of information flows must be adapted to the level of sensitivity of the managed data, depending on the implemented communication resources. The dataflow security ensures integrity and confidentiality of the information being exchanged. The sensitive resources must be secured following the principle of "deep defense" by implementing layered security protection, e.g. data encryption on both application and network layer. Network security must be ensured and controlled according to the criticality of data flows, systems and processes operating within the company computer network infrastructure.

4.6.3 Connection to Internal and External Networks

A system can be connected to the internal networks of ZigZag Global only after sufficient risk analysis is being performed and explicit Information Security approval received, answering the following specifications:

- to be managed in terms of information systems security manner
- must be maintained only by dedicated employees from the IT Department
- direct systems' access, performed by users must ensure adequate user authentication based on the requirements from Access Control Policy

Direct connection between any of ZigZag Global information systems and an external technical environment is strictly forbidden. Any incoming or outgoing connection from ZigZag Global to external networks must be first assessed and approved by Information Security team and answer the requirements for secure architecture with controlled data flows and user access.

4.6.4 Wireless Access Security

Implementation of Wireless Access points in ZigZag Global with access to internal network or services of the company is subject to explicit review and approval by the Information security team and must follow the security principles and hardening.

4.6.5 Software Development Security

Software development process is clearly defined and established by the Business units software development teams, based on the best practices. After performed risk assessment, based on the sensitivity of information which will be managed by the application, the development process includes design and implementation of the appropriate security controls and tests.

The Business units software development teams must be trained in best practices and standards for secure software development lifecycle.

4.6.6 Change Management

All changes must be implemented avoiding conflicts with the information security principles:

- undergo testing, qualification and possibly even IT audit review before deployment
- avoid any interruption and/or denial of service
- be able to be traced and documented
- users who manage the systems must be trained about the changes

Production infrastructure must be logically separated from development and test infrastructures, quality or approval environments. This separation must be strictly observed at the system, application, database and user access profiles' levels. Production changes are only performed after executed, successfully passed and documented technical, functional and security tests (e.g. signoff by CISO), and respectfully signed management approval / validation.

Any sensitive information as part of data used for the test purposes must not contain sensitive real (production) corporate information in clear text, but in scrambled, encrypted or masked format. Any deviation of the above must be immediately escalated to the CTO.

4.7 Physical and environmental security

The resources used to process, maintain and store sensitive information must be located on secure premises and protected by a reliable physical access control. The level of the established physical security must be achieved via appropriate balance between monitoring technologies, preventing unauthorized access, physical intrusion, theft, damage and other distresses.

4.7.1 Environmental Security

The location of computers and other hardware, require appropriate precautions to be taken as preventive measures, against environmental threats like natural disasters and excessive ambient temperature / humidity. The hardware, software

and data, used outside ZigZag Global premises and owned by the company, are subject to the same security principles and protection measures as those applied within the hole corporate environment.

4.7.2 Continuity Management

The business continuity plan of ZigZag Global must describe the resources, organization workforces and activities required for recovery of company business processes in exceptional cases like denial of service, natural disasters, human mistake, etc. The Business Continuity organization-wide plan is regularly tested and updated.

4.7.3 Mobile Computing and Removable Media Management

The use of ZigZag Global removable media, containing sensitive information, inside and outside the company is performed only on authorized employees using authorized hardware devices. Only after employee hieratical supervisor request and validation by BYoD member based risk analysis by Information Security team, the access to external storage drives and UBS Memory Drives is granted.

All sensitive company data must be backed up first and irreversibly removed before the reallocation or scrapping of any technical equipment, mobile devices and/or removable media.

4.8 Technology usage

ZigZag Global requires that the procurement of all information processing facilities be subject to a formal authorization process in respect of information security. “Facility” is defined as “any system(s) or device(s) that will be used to process or store organizational information or that will connect to an organizational network or other information processing facility.” It includes hardware, software and services.

Critical employee-facing technologies just like critical network devices must be featured with adequate authentication techniques. For critical systems, access rights matrixes must be defined, documented, reviewed and updated to ensure that only proper employees are granted access to critical systems and information resources. Any computer System is property of ZigZag Global and is intended to be used explicitly only for legitimate company business. Only persons authorized by ZigZag Global as "Users" may access ZigZag Global Systems and only to the extent that such access is required to assist them in the performance of their work, for as long as it is necessary. All Users shall use organization's computer system in a professional, ethical and lawful manner.

Usage of any kind of private electronic devices is strictly forbidden. Such devices must not be connected to the ZigZag Global internal network of other IT infrastructure. Exception can be made for personal Android and iOS powered mobile phones, which can only be permitted accessing ZigZag Global email. Employees can use their smartphones if:

- Every employee with business need to access ZigZag Global email on his/her mobile device needs approval for corporate CISO / Information Security team;
- Android and iOS devices must be running stock ROMs, cannot be rooted, jail-broken or with bypassed security settings;
- Devices should be encrypted and secured with strong screen lock such as PIN or Password.

For each asset, ZigZag Global IT Department must document sufficient information to identify the asset (type or category of asset, make or manufacturer, model, serial number), identifies the physical (or logical) location of the asset, information security classification of each asset, for each asset, and the security processes or controls (including access controls, backups, etc.) associated with each asset and labels the assets.

Remote access sessions must be automatically disconnected after a specific period of inactivity. Remote access Technologies, used for vendor access to the organization network, must only be connected when required and must be immediately disconnected after use.

Non-public information concerning ZigZag Global, its customers, suppliers or employees may not be transmitted over the Internet unless it is first encrypted in a manner approved by CTO. Any information concerning Card holder data is strictly forbidden to be transferred via Internet.

Public Cloud storage services (e.g. Dropbox, OneDrive, Box.com etc.) are forbidden to be used for corporate data exchange. The only approved public web storage portal for secure sharing of information is the locally hosted OwnCloud/NextCloud portal.Critical and/or sensitive data (for example cardholder data) is strictly forbidden to be sent via email in clear text. In any case it must be approved in written by CTO/Information security team who decides how the data must be protected.

4.9 Operational measures

Preventive, detective and corrective measures required by ZigZag Global are taken under account and applied so that the information security incidents are avoided and cause no impact on any business line of the company.

4.9.1 Incident Management

Information Security Incidents are considered all events (in and outside IT) which might lead or led to breach in Confidentiality, Integrity and Availability of corporate data. Any exception of the normal working processes of data creation, processing or deletion and/or exceptions in information systems workflow at ZigZag Global might potentially lead to a crisis situation.

It must be noted that during the containment and/or investigation of an Information Security incident, the priority must be given (and ensured by the relevant managers) to Information Security tasks over the normal the day-to-day operational activities. The business recovery plans must be formally prepared and ready for execution when needed.

4.9.2 Compliance

The information security strategy is based local legal and regulatory requirements. Compliance with also worldwide best practices and standards for information security (ISO 27001, SAS70, OWASP, GDPR, etc.) is also considered within the information security strategy:

- Local legal and regulatory requirements enforcement (laws, regulations, etc.),
- Respect of industrial property.

5 Roles and responsibilities

Main groups of responsibilities of CISO/Information Security Team concerning the security of company information assets are:

- Information Security Governance–Establish and maintain an information security governance framework and supporting processes, to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly.
- Information Risk Management and Compliance–Manage information risk to an acceptable level to meet the business and compliance requirements of ZigZag Global, local legal acts and regulatory directives.
- Information Security Program Development and Management– Establish and manage the information security program in alignment with the information security strategy.
- Information Security Incident Management–Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact.

6 Enforcement

All individuals that are authorized to use corporate systems, applications, network and originating from the information systems data, are obliged to adhere to all aspects of the Information Security Policy with caution in terms of not exposing the information systems at risk and to report the exceptional security related activities.

Hierarchical management – The hierarchical manager respects, applies and enforces among the staff under their responsibility, ZigZag Global, legal and regulatory requirements and principles related to information security. The

hierarchical manager also ensures performance of permanent supervision and informs the CISO/Information Security Team and Human Resources Department (if disciplinary sanctions are required) for any situations or incidents, exceptional from the normal working process, which can expose the company to security risks.

Technical staff responsibilities – Staff with significant / privileged technical access rights (e.g. IT Administrators, Developers, DB administrators, IT Support, etc.) must respect the security rules and apply the required necessary measures in terms of higher level of information systems security. The IT responsible employees are also responsible for avoiding security related risks that can have impact on the business strategy of the company.

Any exceptions of the policy should be validated by the CTO in advance. Employees who don't adhere to the present policy will face disciplinary action.

7 Glossary

Availability – Information asset of being accessible and usable on request by an authorized entity.

Authentication - The act of verifying the identity of a system entity (e.g., user, system, network node) and the entity's eligibility to access computerized information.

Business Process – A collection of activities influenced by the organization's policies and procedures that takes inputs from a number of sources.

Classification - Definition of the level of sensitivity of a resource according to one or more security criteria.

Confidentiality – Property of information consisting in its being made available only to unauthorized individuals.

Confidentiality Agreement – Acceptance agreement signed for consideration by an external vendor of the data confidentiality during its utilization.

Continuity Management – Preventing, mitigating and recovering of the services from disruption.

Data Owners - Individuals, normally managers or directors, who have responsibility for the integrity, accurate reporting and use of computerized data.

Employee – is a comprehensive notion and may indicate person who has signed temporary or permanent labor contract, civil contract with any of the ZigZag Global subsidiary companies, including trainees.

Information Security - Absence of unacceptable risk and protection of data and systems keeping the threats associated with them at a tolerable level.

Information Security Awareness Program – Planned grouping of dependent actions that includes the full scope of training, business, process, people, technology and organizational activities that are required to achieve a satisfactory level of user knowledge related to information security.

Information Security Incident - An event not being part of the ordinary operation of a service and causing an interruption to, or a reduction in, the quality of that service. The event can potentially affect the confidentiality, integrity or availability of an application or an information system.

Information Security Measure - Activity used to evaluate and communicate performance against expected results. Measures are normally quantitative in nature capturing numbers, money, percentages, etc., but can also address qualitative information such as customer satisfaction.

Information System – Set of means used to collect, process, keep and communicate the data necessary for the purposes and the correct functioning of a company or of a given functional area.

Integrity - Property of information assets and resources consisting in their not being altered or destroyed in an unauthorized manner.

IT - Information technology; the hardware, software, communications and other facilities used to input, store, operate, transmit and output data in whatever form.

Logical Access Control – Limitation of access to information or processing resources by authorized persons.

Non-repudiation – Incontrovertible prove for data authenticity exists.

Risk - Combination of the probability of an event and its consequences such as possibility of loss due to the existence of one or more threats to information.

Threat - Circumstance in which information or information processing resources are liable to be intentionally or accidentally damaged, modified, exposed, inaccessible or affected to the detriment of the establishment.

Traceability – Information systems have the functionality for track of performed by the systems users operations.

Vulnerability - Characteristic of a resource which may constitute a weakness or a flaw with regard to information system security.