Position Green

Information Security Policy

Last updated: 2021-10-20

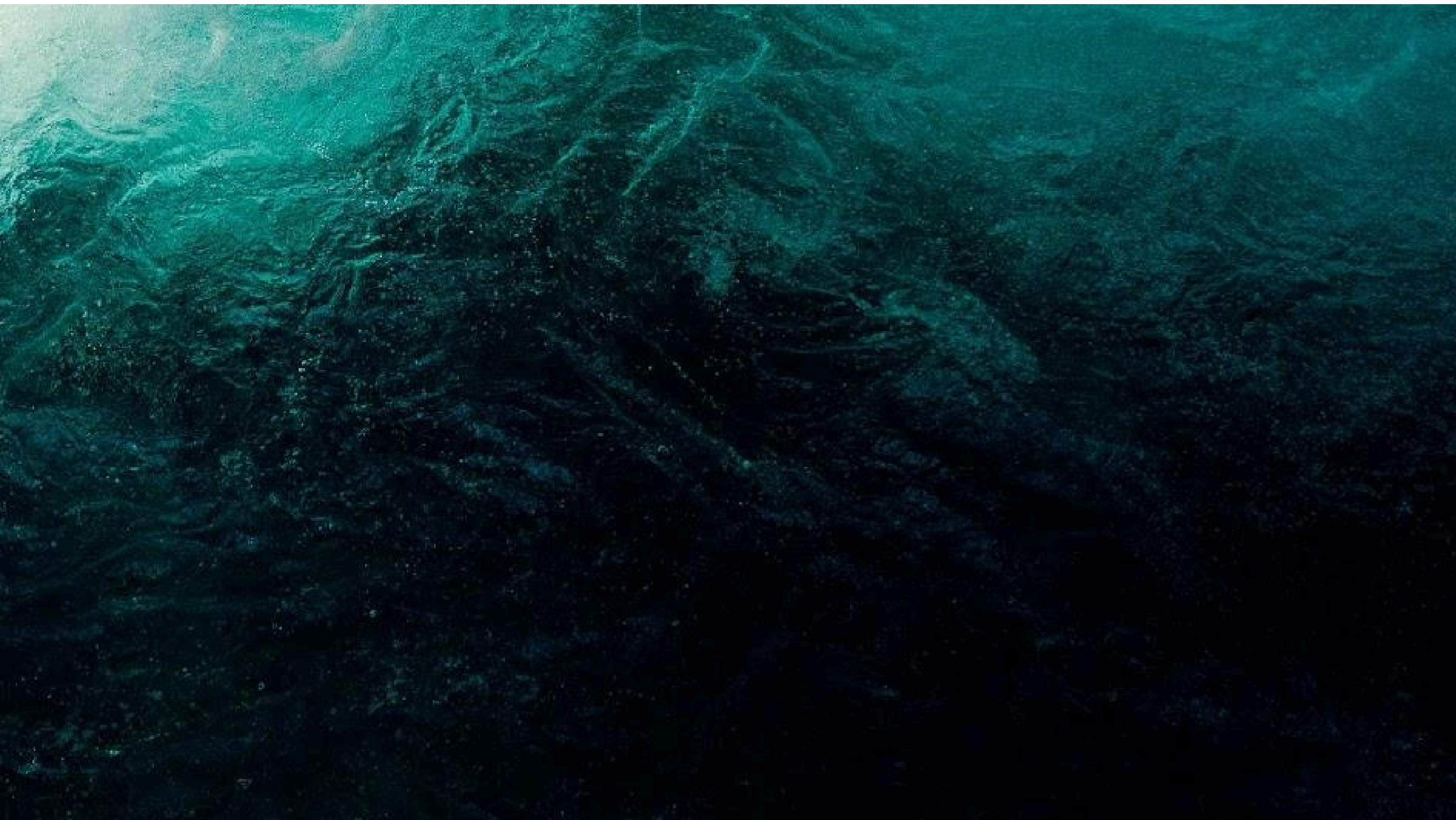

Table of Contents

Purpose

The purpose of this document is to describe the Information Security Policy in Position Green AB. Information security is a continuous process in place to enhance confidentiality, availability, integrity of information and information assets covering all information regardless if it is processed manually or automated.

Overall principles

Position Green’s information security policy can be derived from the following principles:

- Confidentiality - only individuals with authorization can access data and information assets.

- Integrity - data should be intact, accurate and complete, and IT systems must be kept operational.

- Availability - users should be able to access information or systems when needed.

Information Security Guidelines

The following overall principles encompass Position Green's Information Security Guidelines:

- Ensure compliance with current laws, regulations, and guidelines
- Establish controls for protecting Position Green's and our clients' information and information systems against theft, abuse and other forms of harm and loss
- Motivate employees to maintain responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents
- Ensure business continuity even if major security incidents occur
- Ensure the protection of personal data
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by Position Green
- Comply with methods from international standards for information security, e.g. ISO/IEC 27001
- Ensure that external service providers comply with Position Green's information security needs and requirements
- All stakeholders are made aware of Information Security on a continual basis
- All breaches of Information Security are reported and investigated by the Information Security Team
- Information Security Management System is reviewed, updated, and improved periodically

Organization responsibilities

The following parties are responsible for continuously updating the Information Security Policy and the work related with it on a daily basis:

Information Team

The primary responsibilities of the Information Team are to ensure the Information Security Policy is kept up-to-date and updated. They also make sure that all employees of Position Green are aware of the Information Security Policy and introduce it to new employees as part of their onboarding process. Whenever a change is made to the policy, the Information Team informs all relevant parties, presents the changes made and what their practical implications are.

Change Control Board

Any change to Position Green's SaaS platform that affects or may have impact on network infrastructure, security or the managing of information must be presented to the Change Control Board. This includes new hardware or changes to the hardware that Position Green is using.

Information Security Team

The Information Security Team is responsible for prioritizing a reported incident based on its severity and deciding upon actions required to resolve it. They are also responsible for conducting analysis and set plans with the purpose of preventing similar incidents from happening again.

Security Incident Management

Position Green follows the ISO/IEC Standard 27035 procedure:

- Prepare to deal with incidents e.g. prepare an incident management policy, and establish a competent team to deal with incidents.

- Identify and report information security incidents

- Assess incidents and make decisions about how they are to be addressed e.g. resolve and get back to business as quickly as possible. It also includes, when required, collecting forensic evidence, even if it delays resolving the issues.

- Respond to incidents i.e. contain, investigate and resolve them.

Learn the lessons - rather than simply identifying what could have been done better, this stage involves carrying out changes that improve the processes within an immediate time frame.

Security Incident Process

When an incident is detected and reported it is assessed by the Information Security Team. Incident prioritization is based on the severity of the incident. Depending on the severity, follow-up actions may differ.

When further incident investigation is needed, a responsible person is appointed to continue gathering additional information required to decide upon what follow-up action to take.

If the issue is well known and no further investigation or analysis is required, the Information Security Team takes immediate action to resolve it.

After the incident has been resolved it is once again brought up to the Information Security Team to present a post mortem and propose any routine changes to avoid or mitigate similar incidents from happening again.

All incidents must be documented and stored on GSuite with the appropriate permissions. If an incident pertains to a specific client, the client must be informed about the incident and what actions have been performed to resolve the incident within 24 hours.

Disciplinary routines

All employees are obligated to report suspicious behaviour to the Information Security Team who shall initiate relevant investigations and actions/reporting. Disciplinary sanctions following information security breaches are determined from case to case. If crime has been committed, the authorities are contacted immediately.

Confidentiality

Only individuals with authorization can access data and information assets.

Authentication and Authorization

All systems in Position Green must support OpenID Connect and integrate with Position Green Access and Identity Provider. This includes where authentication flow involves the user directly or if it is a system-to-system communication.

All role-based authorizations must use the claims from the access token verified by the certificate of the identity provider.

Management of Information Assets

Classification

All structured information required by Position Green shall be documented and classified to determine the classification of data. If a change of requirements would occur, e.g. making it mandatory for a user to enter sensitive personal data, the change would be required to be proposed to the Change Control Board and necessary actions would be undertaken depending on the urgency and necessity of the requirement change.

Security

Describes the security policies in Position Green.

Office

Position Green HQ in Malmö requires a tag with a PIN code to access the room. When leaving the office all employees must lock their computers into their cabinets before leaving. All cabinets are located in rooms with motion detectors connected to a central alarm system. When an employee leaves the workplace, he/she shall verify that no confidential or sensitive information or media is left unguarded. Such items shall be stored in a protected and locked cabinet. Employees are not allowed to leave confidential documents by printers or any shared space such as desks or in regular bins. A security company patrols the office premises outside of office hours.

Any visitor must be escorted to and from the building.

The last person to leave the building is responsible for setting the alarm. The building is under surveillance by a security company outside of office hours.

Data Center

Access to the data center is restricted to only those selected employees with System Administrator privileges that require access to it. The data center must be placed in a remote site and on a separate network. Position Green has outsourced its data center to Bahnhof's facilities in Malmö, employing their high security standards and data center availability.

Devices

The following principles are operating system and vendor independent:

- To access Google GSuite 2-factor is required by domain policy and must be supported on the device
- Any computer (laptop or workstation) must have its hard drives encrypted
- Firewalls should be enabled per default
- Anti-virus or malware software should be enabled per default

Integrity

Data should be intact, accurate and complete, and IT systems must be kept operational.

Data

Any data stored by an application must use ACID (Atomicity, Consistency, Isolation, Durability) transactions. This is to ensure the integrity and accuracy of the reported data. Relationship and index constraints should be used to guarantee the data never can be incomplete.

Encryption Management

Provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory, and contractual requirements. Keys should not be reused for different purposes.

Keys and encryption should be reviewed regularly to make sure no algorithm used has been deprecated and replaced with a new recommendation.

Encryption methods for live data at rest

Live data should be encrypted by at least AES128 when it is live in a system. If a hardware solution is available it should be used.

Encryption methods for data in motion

Any traffic from and to Position Green should be encrypted. Web traffic should be at least TLS 1.2. Certificates should have an rotation max length of 3 months.

Encryption methods for backup data at rest

Data stored as backup should be encrypted by at least AES256.

Encryption methods for secrets

Any secrets used by systems should be encrypted by at least AES128.

Operations

Logs

Logs must be shipped to our central logging system. If application log then use XID to be able to track requests between systems. Operating systems should be configured to send their logs per default. Source must be set to an identifiable and consistent name for traceability.

Monitoring

All systems must be monitored for system resource utilization (minimum cpu, disk, memory). Recommended is to expose application specific metrics to ensure we can monitor specific use cases. Metrics should be exposed using Open Metrics Standard.

Alerting

Whenever a new metric is introduced it should be assessed if an alert is required and at what threshold. Alerts must be reviewed and thresholds updated after an incident has been alerted, in order to avoid a situation where we receive too many alerts requiring no action.

Destruction

Computer equipment and media must be wiped or disposed of securely as soon as they become redundant or no longer required. The method used will depend on the nature of the processed data in accordance with Information Security Team guidelines.

Availability

Users should be able to access information or systems when needed.

Capacity planning

By using the information gathered from the monitoring systems we can perform evidence based capacity planning. A threshold for system utilization should be set and updated, and whenever it is reached the situation should be assessed for what subsequent action needs to be taken. This threshold must be set to a level that is low enough for us to take actions and increase the capacity in a timely manner. We must never be in a situation where we are unable to onboard new clients because of capacity issues.

Disaster Recovery

All systems must have automatic scripts for configuring and setting up the system. Any manual step must be documented. Configuration for each environment must be separated.

The Recovery Time Objective (RTO) is 4 hours and the Recovery Point Objective is 24 hours.

A simulated disaster recovery should be conducted annually to test RTO and RPO.

Exceptions

Information Security Policy exception requests must be submitted to the Information Security Team.

Requests will be assessed and if there is no other solution but to approve the exception it must be for a limited time constraint. When the time period for the exception has come to an end it must either be re-submitted and re-evaluated by the Information Security Team, or removed completely.

Any exception must be documented in GSuite under the Information Security Policy/Exceptions folder.

Each exception must include the following information:

- Title
- Description
- Owner
- Decision
- Time limit

Risk

Risk management concerning information is important. This involves identifying important information assets. The information risk management also includes GDPR regulations and compliance at Position Green, for more information regarding GDPR see General Terms and GDPR.

Information assets at Position Green

- Customer Data (database and files)
- Documentation and training materials
- Source code
- Operational data (logs)
- Contracts

The information asset owner is the CTO at Position Green and works together with the Information Security Team.

Annually there should be a review of the identified assets and the categorization of classification to make sure each gets sufficient resources to mitigate any risk.

It is the responsibility of the CTO to ensure the training material in our LMS is up-to-date.