Policy for information security and environment

Table of Contents

Environmental Policy

Introduction

For iSOC24 B.V. (in this document names iSOC24) Corporate Responsibility means more than just to comply with law and legislation. Within the manifest three long term ambitions have been formulated:

1. We are a people-oriented organization: we strive for high ratings from both customers and employees.
2. We are a social organization: we want to create value for our customers with simple and responsible products and services.
3. We are a sustainable organization: we work towards a climate-neutral organization, whereby we make our own business operations more sustainable and actively stimulate customers to save energy.

Corporate Responsibility also means that we consider all the consequences of our actions. Nature and the environment must be protected and human rights must never be violated. We take this into account when making investments and in our internal business operations. We expect the same from our suppliers. Together we want to work on a sustainable purchasing process by thinking proactively about sustainability.

Implementation of the environmental management system (ISO 14001)

iSOC24 acknowledge the need to focus more on the environmental impact of its activities. For this we have setup and implemented an environmental management system according to the ISO 14001 requirements, in order to further control and where possible reduce environmentally harmful activities. Opportunities have already been identified for this with regard to waste separation, reduction of paper use, reduction of fuel use, the use of more environmentally friendly / sustainable products, making housing more sustainable and motivating partners and suppliers to take greater account of the environment.

- iSOC24 has an environmental management system (ISO 14001 environmental certification).
- iSOC24 has an environmental program which includes:
    - Reducing CO_2-emissions from business operations.
    - Reducing the use and/or replacement of materials and materials that are harmful for the environment.
    - Reducing water use.
    - Reducing electricity.
    - Reducing and recycling waste.
- iSOC24 has a policy for sustainable purchasing.
- iSOC24 reports on progress and audits it externally.
- iSOC24 reduces the impact on the environment with its measures.
- iSOC24 takes social interests into account.

Information Security

Introduction

Information Security is extremely important to iSOC24. Securing your data is one of our top priorities. We support transparency about our security principles and are happy to help you understand our approach.

Our security is aligned with the ISO 27001 standard and is regularly checked and assessed by third parties.

Security of Personnel

Security controls regarding personnel apply to all temporary and permanent internal and external employees and suppliers who have access to iSOC24, its internal information systems and/or access to iSOC24's office space. Before granting access to systems, all employees must agree to a non-disclosure agreement, pass a background screening, and attend security training. This training covers privacy and security topics, including device security, acceptable use, malware prevention, physical security, data privacy, account management, password management and incident reporting. Upon termination of employment, all access to systems will be immediately disabled.

Security and privacy training

During employment all employees must refresh their knowledge of privacy and security at least once a year. Employees sign that they have read and adhere to the information security policy documents. Some employees, such as administrators and support staff, who have additional access to systems or data, receive additional work specific training on privacy and security. Employees are required to report security and privacy issues. Employees have been informed that non-compliance with policies may have consequences up to termination of employment.

Assigned security professionals

iSOC24 has defined roles and responsibilities to determine which roles in the organization are responsible for the operation of various aspects of its Information Security Management System (ISMS). The responsibilities of each role are detailed in our security documents. iSOC24 has appointed an ISMS Manager with overall responsibility for the implementation and management of its ISMS.

Policy and standards

iSOC24 maintains a set of policies, standards, procedures and guidelines that show employees how to use our ISMS. Our security documents ensure that our customers can rely on our employees to behave securely and ethically. The policies are living documents: they are regularly reviewed and updated and, if necessary, made available to the employees to whom they apply.

Audits, law- and legislations, and third-party assessments

Audits

iSOC24 evaluates the design and operation of its ISMS for compliance with internal- and external standards. iSOC24 is assessed by external auditors. Audit results are shared with management and all findings are followed up.

Legal Compliance

iSOC24 employs dedicated legal and compliance professionals. These professionals are embedded in the development cycle and assess products and properties whether they, meet the legal requirements.

Protection of customer data

The focus of iSOC24's security program is to prevent unauthorized access to customer data. To this end, our team takes comprehensive steps to identify and mitigate risks, implement best practices and continuously evaluate to improve.

More information about our Privacy Statement can be found on our website.

Network security

Rules have been drawn up within iSOC24 for sending information over public networks. The level of security and the way of sending information is determined by the assigned classification of the information.

Classification and storage of data

Within iSOC24, information is classified according to the following criteria:

- Value of the information based on the impact assessed during risk management.
- Sensitivity and criticality of information based on the highest calculated risk for each item during risk assessment.
- Legislation and contractual obligations based on the List of Laws, Regulations and Contractual Obligations.

A distinction is made between classification levels where each classification level is linked to a set of security measures.

Authorized access

To minimize the risk of data exposure, iSOC24 follows the principle of *need to know*. Employees only have access to information that they reasonably need to perform their current duties. To maintain this, iSOC24 applies the following controls:

- Each user's access is regularly reviewed to ensure that the access granted is still appropriate for the user's current work responsibilities.
- To further reduce the risk of unauthorized access to data, iSOC24 applies, if possible, two-factor authentication for access to third party systems.
- iSOC24 requires personnel to use an approved password manager. Password managers generate, store and enter unique and complex passwords. Using a password manager helps prevent password re-use, phishing, and other risky behaviour that can reduce security.

System monitoring, logging and alarms

Within iSOC24 roles and responsibilities have been established for both checking the logs of automatically reported errors and for recording errors reported by users to analyse why errors occur and to take appropriate corrective actions.

Bring Your Own Device (BYOD)

iSOC24 supports the use of BYOD for business use. This only applies to employees who otherwise would not be able to perform their work. A registration is kept with the names of employees who are allowed to use BYOD along with the applications and databases that they are allowed to access with their own devices. In addition, iSOC24 sets several rules for using BYOD and requires a minimum configuration for each device.

Responding to incidents

Any employee, supplier or other third party that comes into contact with information and / or systems of iSOC24 must report any threat, incident or event to a system that could lead to a possible incident to the ISMS Manager. Various procedures have been developed to respond quickly and adequately to incidents. All incidents are regularly reviewed and evaluated to learn from them.

Disposal and destruction of equipment and media

Within iSOC24 rules are in place regarding the removal and / or destruction of equipment and media before it is discarded, sold, donated, shipped, repaired, re-used or given to another user.

Clear desk & clear screen policy

Within iSOC24 we follow a clear desk and clear screen policy. This means that if the authorized person is not at the workplace, the person must remove the information, papers, storage media, from the desk or other places such as printers, copiers, etc. to prevent unauthorized access. Likewise, all sensitive information should be removed from the display and a screen lock must be applied when the authorized person leaves the workplace.

Business continuity

iSOC24 has drawn up various plans and procedures that ensure that its business continuity is guaranteed.

Third parties

To run the business efficiently, iSOC24 relies on third party services. If third parties may influence the service of iSOC24, iSOC24 takes measures to ensure the same level of security is guaranteed. iSOC24 has agreements with third parties that require them to comply with the obligations that iSOC24 has set for themselves. If necessary, iSOC24 audits the effectiveness of the organization’s security controls at least once a year.

Conclusion

At iSOC24 we take security seriously because everyone who uses our services may expect from us that their data will be kept safe and confidential. Security of this data is a critical responsibility we have to our customers and we work hard to maintain that trust.