Ecochain Security

Information Security Whitepaper

Ecochain

Content

Introduction

The Ecochain application is a Saas tool designed and built in-house to deliver powerful portfolio insights in the domain of sustainability.
This policy, which is based on the ISO/IEC 27002:2013 code of practice, outlines Ecochain's approach to security and compliance including organisational and technical controls regarding how we protect your data.

1. Information security organisation

At Ecochain we have strict controls around the organization and access to information.

1.1.1 Internal organisation

Security-related roles and responsibilities are defined on an organisational level and each employee is assigned only enough access to perform their role. Employees responsible for organisational security have special clearance and access, and they can assign, audit and control access for the rest of the organisation.
When starting projects, whether consulting or internal, an information security risk analysis is performed to determine if any new controls are required.

1.1.2 Mobile devices and teleworking

Storage of client information or any other sensitive organizational information is strictly forbidden on mobile devices.
In the case of laptops or other devices that can be used remotely, we have strict policies regarding their use.
For instance, all client or organizational information is kept on a folder synced with a secure file server. Hard drives are encrypted to protect against intrusion. Users accounts are locked out automatically after a short time. Malware protection is installed on all devices.
When working remotely, our employees will sometimes have limited access to certain aspects of our business. This is to safeguard sensitive areas of our infrastructure.
For instance, administration of our core Saas applications can only be done from within a secure location.
When using public networks, it is required for our employees to use a secure VPN service to access any Ecochain or client services.

2. Human resource security

We have a strong focus on security in Ecochain. From the hiring process to day-to-day activities, a large emphasis is placed on security awareness.

2.1.1 Prior to employment

All employees and contractors are required to sign a non-disclosure agreement prior to gaining access to information. Employees are also required to adhere to a [code of conduct]

2.1.2 During employment

All employees receive ongoing security training. As part of our commitment to our customers to keep their information secure, we continuously share knowledge internally and focus security awareness on password management, phishing, secure device management and privacy.

Our engineering team includes security and privacy specialists. They are responsible for maintaining the application and infrastructure security, performing security reviews, monitoring for security threats, implementing quality assurance measures and performing penetration tests.

2.1.3 Termination and change of employment

Ecochain makes use of internal workflows to onboard, off-board or change roles for employees. This provides for access management based on function. When an employee is no longer required to fulfil a role, access is revoked and assets returned.

3. Asset Management

Assets are an important part of managing information security, and at Ecochain we've put strict procedures in place to manage all types of assets.

3.1.1 Responsibility for assets

We have an internal inventory of all assets, be it devices, software or other that can be purchased, transferred and participate in the flow of information. These assets are all controlled in a workflow system to make it clear who has ownership and to whom it is currently assigned. Devices that store data are physically destroyed when they have reached end of life.

3.1.2 Information classification

Ecochain defines all client related information as highly sensitive. This removes the need for classifying specific types of information and assigning different types of procedures and controls.
Access restrictions are placed on all levels, and employees are only granted access to relevant areas.

3.1.3 Media handling

When not in use, any storage media, devices or paper is locked away in a secure location.
When devices or media is transferred between employees, or disposed of, any data present is first made unrecoverable.
In the case of disposal, the media is physically destroyed, whether in electronic or paper format.

4. Access control

4.1.1 Business requirements of access control

Access to systems within the organisation is limited to those employees directly involved in that area, and then specific access is limited to their function.
In general, the concept of least-privilege is used to determine the absolute minimum level of access required to perform their function.

4.1.2 User access management

Each Ecochain employee receives a unique user ID linked to all systems. No shared ID's are used. Part of out on-boarding, role-change and off-boarding processes are assignment, change and revocation of roles linked to the relevant user ID. These roles determine the level of access the user has to different systems within the organization.
All administrative access to servers are firewall and SSH key protected so that it can only be accessed by specific employees from a specific IP address.

4.1.3 User responsibilities

We have a strict password policy, e.g. passwords should be unique per system and master passwords should conform to minimum length and complexity rules.
SSH keys or passwords are never shared between employees.

4.1.4 System and application access control

For all business-critical applications, we require the use of 2-factor authentication.
As much as possible we also use a centralized user management system to define roles specific to employees, which in turn controls which systems and functions they have access to.
We make use of a centralised system to manage secret authentication information (e.g. passwords or SSH keys) for all Ecochain employees. Each employee manages their own information, and access to shared groups are controlled by an administrator.
Access to this system requires 2-factor authentication.
Each employee's authentication information is kept separate from other employees.
Authentication information is never recorded in any other system, paper or device, except for the management system.
Access to source code is strictly controlled and limited to only developers. Each developer is provisioned with their own SSH key to gain access, and depending on their function they might have restricted access to some parts.

5. Cryptography

5.1.1 Cryptographic controls

Cryptographic controls in Ecochain applies to:

- Ecochain premises where electronic data might be stored;
- Third parties with access to sensitive Ecochain or Ecochain client data;
- Employees or contractors using Ecochain systems;
- Information system resources including networks, servers, personal computers, mobile devices owned by Ecochain or authorised to access Ecochain data networks.
- Electronic Information of a sensitive or critical nature to Ecochain or its clients.

All sensitive data transferred outside of Ecochain systems are encrypted.

All sensitive data are encrypted at rest on any servers, whether on-premises or hosted by third parties.
All hard drives on personal computers in use by Ecochain employees or contractors are encrypted.
Mobile devices are protected by passwords or pin numbers.
When accessing Ecochain systems over public wifi, an encrypted VPN channel must be used by employees or contractors.
Cryptographic keys in Ecochain are generated within cryptographic module with at least a FIPS 140-2 compliance. Where such keys are used in source code, they are stored securely.

6. Physical and environmental security

6.1.1 Secure areas

Our Ecochain offices are locked and protected by an alarm connected to manned response.
Each employee has a unique code for entry, and the office is divided into separate areas which are locked after hours.

6.1.2 Equipment

The office does not contain any servers or hosting facilities, and personal computers are locked away in a secure cupboard when not in use.
All personal computers and mobile devices are required to automatically lock after a short amount of time.
At our offices, we have a clean desk policy to minimise the risk of printed information being compromised. Furthermore, any sensitive documents are shredded immediately after use.

7. Operations security

7.1.1 Operational procedures and responsibilities

We have a dedicated operations team that take care of all infrastructure concerns, including:

- server setup and installation
- server patches and upgrades
- software release management
- infrastructure and software monitoring

Our production environment is completely separate from other environments, where development and testing occurs. Any changes to the production environment are first tested on other environments.

7.1.2 Protection from malware

Having our documents stored on Google drive means automatic virus scanning.
Thus far, we're not supporting document uploads to our Saas product, but if we were it would be coupled to a virus scanning system.
All of our employees are trained, as part of their security training, to avoid dubious websites, only install software from accredited sources, and identify and remove phishing emails.

7.1.3 Backup

Operational data is backed up as part of the operating agreement with third parties.
Our Saas product data is backed up automatically as part of the RDS provisioning with AWS.
The current backup policy is daily with a 10-day retention time.

7.1.4 Logging and monitoring

We keep detailed logs of system events, including:

- system errors
- security related state changes
- user events

Sensitive user data is never captured during logging.
Logs are used to monitor system activity as well as assisting to resolve issues.
Only the core operational team has access to logs.

7.1.5 Control of operational software

Our dedicated operations team are tasked with maintaining the operational livelihood of our infrastructure. This includes patching servers to keep abreast with security fixes, and controlling the release cycle of our Saas application.

7.1.6 Technical vulnerability management

Our operations team subscribe to relevant feeds of security notices and will do a risk assessment on each posted vulnerability to determine a course of action.
Refer to the Patch Management Policy for more information

7.1.7 Information system audit considerations

Security is an ongoing process and should be tested and audited continuously as threats and countermeasures change over time.
Our systems have been penetration tested by third-parties and we regularly do our own penetration tests too.
Internally we review processes on a regular basis to ensure they are up to date.

8. Communications security

8.1.1 Network security management

Our server infrastructure has been designed and configured with prevention in mind.
For example, the servers aren't directly accessible from the web but are protected by a VPC (virtual private cloud) and an internet gateway that only accepts certain types of connections.
Only the web servers allow connections through the internet gateway from outside.
Internal servers like databases are not at all accessible from outside the VPC, but only from trusted servers and applications inside the VPC.

8.1.2 Information transfer

Our servers support strong encryption protocols such as TLS to secure connections from customer devices. The Saas application encrypts all transferred data on the wire.
All Ecochain employees receive training regarding safe and responsible use of electronic messaging.
Furthermore, it's company policy to use 2-factor authentication when logging into email accounts. This mitigates risk of email accounts being hacked into.

9. System acquisition, development and maintenance

At the time of publication, Ecochain offers a single Saas application consisting of different features available to divergent business types and users.
All controls pertaining to information systems, development and test data are specific to the above mentioned Saas application.

9.1.1 Security requirements for information systems

Requirement analysis for new features always involves security specialists to determine whether new functionality has an impact on the standard operating procedure of the software.

9.1.2 Security in development and support processes

Ecochains development process follows secure development best practices. Part of this process is design reviews by peers and security specialists, risks assessments, static code analysis and recurring penetration testing performed by security experts.
Changes to Ecochain infrastructure are logged, tested and documented. These updates are performed regularly to minimise the impact on our customers. Whenever large upgrades are planned, and significant outage or impact to clients are expected, Ecochain will always communicate such activities ahead of time. Such changes are done during regular change windows where system use is at its lowest.
Changes to infrastructure or software are always reviewed beforehand, approved by business and tested during and after implementation.

9.1.3 Test data

Our test and production environments are completely separate, including data being used.
Test data is produced internally and structured to test all relevant scenarios applicable to the application.

10. Supplier relationships

Effective relationships with suppliers are critical to the continued success of Ecochain. As such it's very important for us to understand the security constraints of our suppliers in order to mitigate the risk to our clients.

10.1.1 Information security in supplier relationships

Information security requirements vary according to the type of interaction with each supplier. But in general:

information security requirements and controls are documented;

NDA's are used where applicable;

due diligence is performed when selecting suppliers;

access by suppliers to Ecochain data and infrastructure are limited as much as possible;

suppliers are expected to exercise adequate control over information security policies used with sub-contractors or parties in their supply chain.

In cases where we store client data on supplier infrastructure, we require data to be encrypted at rest, with a minimum encryption strength of AES-256.

10.1.2 Supplier service delivery management

Changes to supplier policies are monitored on a regular basis to ensure they are still fit for purpose.

11. Information security incident management

Ecochain recognises the importance of and is committed to, effective security incident management in order to protect the confidentiality and integrity of our customers' information assets.

11.1.1 Management of information security incidents and improvements

Ecochain has monitoring in place on infrastructure and our incident management team are able to diagnose business impacting issues.

Incidents are categorised and prioritised according to their impact and severity. Any incident involving customer information is given the highest priority, and the customer would be notified immediately, while it is being resolved.

12. Information security aspects of business continuity management

At Ecochain we place a high value on the ability for our customers to rely on the continuous use of our services.

12.1.1 Information security continuity

Our network infrastructure and application is designed to be resilient and highly available and we're continuously improving on areas such as scalability and fault tolerance.

12.1.2 Redundancies

Infrastructure uptime is monitored continuously and failure is automatically reported to the infrastructure team who is responsible for uptime of the system. Backups of data are made daily, should any need arise to rebuild the database.

13. Compliance

13.1.1 Compliance with legal and contractual requirements

Ecochain complies with all local and international laws applicable to the use of our software.

13.1.2 Information security reviews

Ecochain undergoes periodic information security reviews internally and externally by independent parties. This is done to measure the effectiveness of controls in place and ensure continuous improvement.

Technical reviews are performed on a continuous basis involving:

- vulnerability assessments
- penetration tests
- architecture reviews
- policy reviews

Ecochain

Ecochain Technologies B.V.
Burgerweeshuispad 201
1076 GR Amsterdam

+31 (0)20 303 5777
www.ecochain.com