

Information Security Policy

Version 1.0

Green Platform N.V. (hereinafter “Green Platform”, “Company”) has a duty to protect its information assets, ensure business continuity and protect the flow of information, internally and externally. Information security is vital to ensure effective and protected data sharing, at the same time protecting the information infrastructure from security incidents.

The Green Platform Information Security Policy is intended to safeguard the Company, Company staff, its clients, partners and owners of intellectual property rights from information security related incidents and any consequential action, loss of income or damage. The Policy also aims to establish control requirements on network systems, based on the International Standards ISO/IEC 27001 and ISO/IEC 27002.

1. Scope

This Policy applies to all the following groups of staff and affiliates at Green Platform (but is not limited to):

Anyone accessing **information** that is the property of Green Platform;

Anyone accessing the Green Platform **computer network**;

Anyone using computer equipment that is the property of Green Platform;

All Green Platform **staff**;

All Green Platform **affiliates and providers**.

This Policy protects information systems used to store and process information.

This includes, but is not limited to:

- Cloud systems developed or commissioned by Company;
- systems or data attached to Company networks;
- systems managed by Company;
- mobile devices used to connect to Company networks or hold Company data;
- data over which Company holds the intellectual property rights;
- data over which Company is the data controller or data processor (wherever held).

2. Responsibilities

It is the responsibility of all users of Company information sources and systems to comply with Company instructions regarding the safeguarding of information.

The Company will make this Policy available to all new staff. The Company will make staff aware of the Policy and inform them of any significant revisions to the Policy.

The Company understands its responsibility for managing information correctly. Such information management promotes business efficiency (recognising information as a primary asset, worthy of protection), effective risk management, legal compliance (especially in relation to the General Data Protection Regulation) and sound corporate governance.

Responsibilities of the staff, Company`s affiliates, suppliers and partners:

All staff of Company, Company's affiliates, suppliers and partners, third parties will be users of Company information. This carries with it the responsibility to abide by this Policy, supporting policies and relevant legislation. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. To report data breaches, please see Section 3.6: Incident Handling

Business Led Technology Teams:

Responsible for the information systems (e.g. HR/ Registry/ Finance) both manual and electronic that support Company's work. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

Project managers:

Responsible for the security of information produced, provided or held in the course of carrying out realization of projects. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and mitigated, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms.

Professional service leads, Departmental managers / Line managers:

Responsible for specific area of Company work, including all the supporting information and documentation that may include working documents/ contracts/ staff information.

Data Protection Officer:

Responsible for data protection and records retention issues.

Cyber Security Team:

Responsible for ensuring that the provision of Company's IT infrastructure, cloud environments and applications is consistent with the demands of this policy and current good practice. Responsible for assurance activities, pen testing, information security policies and specialist information security advice. Incident response for cyber security issues. User awareness.

Management Board:

Responsible for approving information security policies.

3. Policy

3.1. Information security principles

The following information security principles provide overarching governance for the security and management of information at Company:

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see Section 3.3. Information Classification) and in accordance with relevant legislative, regulatory and contractual requirements.
2. Users with responsibilities for information (see Section 2. Responsibilities) must:
 - a. ensure the classification of that information is established;
 - b. must handle that information in accordance with its classification level;
 - c. must abide by Company's policies, procedures, and any contractual requirements.

3. All users covered by the scope of this policy (see Section 1. Scope) must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. Access to information will be on the basis of least privilege and need to know.
5. Information will be protected against unauthorized access and processing.
6. Breaches of this policy must be reported (see Section 3.6. Incident Handling).
7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual external audits and penetration testing.
8. Explicit Information Security Management Systems (ISMSs) run within the Company will be appraised and adjusted through the principles of continuous improvement.

3.2 Legal & Regulatory Obligations

We store and process your Personal Data in data centres around the world, wherever Green Platform facilities or service providers are located. As such, we may transfer your Personal Data outside of the European Union. Some of the countries to which your personal data may be transferred for these purposes that are located outside the EU do not benefit from an adequacy decision issued by the EU Commission regarding protection afforded to personal data in that country. Details of these specific countries can be found here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. If we do transfer your personal data outside of the EEA, within the group or to our business partners, we will take all reasonable steps to ensure that adequate measures are applied to keep your personal data as secure as it is within the EEA and in accordance with this Privacy Policy, by relying on the use of standard contractual clauses or binding corporate rules or any other acceptable method that ensures protection of your data based on the standard required within the EEA.

You can always contact us to receive the full list of our service providers outside the EEA which process your data.

3.3 Information Classification

1. The following table provides a summary of the information classification levels that have been adopted by Company and which underpin Company's principles of information security.
2. Information may change classification levels over its lifetime.

Security Level	Definition	Examples
Confidential	Normally accessible only to specified members of Company staff. Should be held in an encrypted state outside Company systems; may have encryption at rest requirements from providers.	Personal Data that used by the Company for KYC/D under requirements of AML policy.
Restricted	Normally accessible only to specified and/or relevant members of Company staff or Affiliates.	1. GDPR-defined Personal Data; 2. Name, email; 3. Reserved committee business; 4. Agreements terms and conditions; 5. Systems; 6. Internal correspondence;

		7. Company policy and procedures (as appropriate to the subject matter).
Public	Accessible to all members of the public.	Information available on the Company website or through the Company's social networks.

3.4 Suppliers and Affiliates

All Company's suppliers and affiliates will abide by Company's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance.

This includes:

- when accessing or processing Company assets, whether on site or remotely
- when subcontracting to other suppliers.

3.5 Compliance, Policy Awareness and Disciplinary Procedures

1. Compliance with this Policy is mandatory.
2. Mandatory user awareness training will accompany this Policy.
3. All current staff and other authorised users will be informed of the existence of this Policy and the availability of supporting policies.
4. Any security breach will be handled in accordance with all relevant Company policies, including appropriate disciplinary policies.

3.6 Incident Handling

1. If a member of the Company's staff is aware of an information security incident then they must report it to the legal@vegangster.com.

3.7 Review and Development

1. This Policy will be updated regularly to ensure it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.
2. Additional policy may be created to cover specific areas.