

VentureGamez N.V.

**Information Security
Policy**

MAY 2025

1. Introduction

Welcome to Venturegamez N.V., a limited liability company, registered and incorporated under the laws of Curaçao, with company registration number 162316 and having its registered address at Kaya W.F.G, Jombi, Mensing 24 Unit A (referred to as "we," "us," or "our" "Venturegamez") Information Security Policy.

Venturegamez is committed to ensuring the confidentiality, integrity, and availability of its information assets, systems, devices, and networks. To achieve this, Venturegamez has established this Information Security Policy (Policy), which defines the security measures, rules, and responsibilities necessary to protect these critical assets.

The Policy also ensures compliance with applicable legal, regulatory, and contractual obligations while preserving the trust of our clients, partners, employees, and stakeholders. Furthermore, it covers specific rules for device management, social media use, internet access, and cybersecurity measures, vital for preventing security breaches and minimizing operational risk.

By accessing company systems, devices and resources all employees, consultants, partners and third parties acknowledge that they have read, understood, and agreed to comply with this Information Security Policy.

2. Scope

This policy considers all information and assets in both physical and digital formats, including but not limited to hardware, software, databases, intellectual property, internal and external communications, and internal business records and applies to all employees, contractors, consultants, and third-party vendors with access to Venturegamez's information, IT systems, or networks.

3. Information Security Objectives

Venturegamez's key information security objectives are to:

- **Confidentiality:** Protect sensitive and confidential information from unauthorized access, ensuring that data is only available to those who are authorized and following the minimization and necessity principle.
- **Integrity:** Safeguard data from unauthorized alteration or corruption, ensuring its accuracy and consistency.

- **Availability:** Ensure authorized users have timely and reliable access to the required information and systems when necessary.
- **Resilience:** Develop and maintain adaptive systems, processes, and protocols to swiftly detect, respond to, and recover from incidents or threats, ensuring minimal operational impact and preserving business continuity in the face of potential disruptions.

4. Governance and Compliance

Venturegamez is committed to adhering to all relevant national and international legal and regulatory requirements, including those related to information security, data protection, and privacy laws. Any non-compliance with these laws will result in severe consequences, including disciplinary actions and possible legal proceedings.

5. Technology and Device Management Guidelines

The use of technology and device management during business hours should be governed by the following guidelines:

- **Devices Usage:** Work devices, including laptops, tablets, and smartphones, are strictly for authorized business purposes only, whether used in the office or during remote work. Any personal use of company devices must be minimized and comply with company policies.
- **Secure Storage:** Devices must be securely stored when not in use. This includes physically locking devices in a secure drawer or cabinet or using strong, complex passwords to lock devices when left unattended, ensuring that unauthorized access is prevented at all times.
- **Lost or Stolen Devices:** In the event of a lost or stolen device, it is mandatory to report the incident immediately to both the police and the IT department, as well as the IT Department at Venturegamez. The device must be remotely wiped as soon as possible to prevent any potential data breaches or unauthorized access.
- **System Updates:** Employees are required to install mandatory system and security updates on company devices immediately upon notification. These updates are critical to protect devices from security vulnerabilities, safeguard sensitive data, and maintain overall system integrity.

- **Shutdown Policy:** To minimize the risk of unauthorized access or data breaches, employees must shut down their computers and mobile devices at the end of each workday or during extended periods of inactivity, ensuring that devices are not left exposed to potential threats.
- **Screen Locking:** Devices and workstations must be configured to automatically lock after no more than ten (10) minutes of inactivity. Employees must also manually lock their devices whenever they leave them unattended, further securing access to sensitive information.
- **USB and Removable Media Protection:** Data stored on removable media (e.g., USB drives) must be encrypted, and devices should be scanned for viruses or malware before being connected to company systems. Employees are strictly prohibited from using unauthorized removable devices (e.g., personal USB drives, external hard drives) to mitigate the risk of malware introduction and data breaches.
- **Mobile Device Security:** Mobile devices must be secured with strong passcodes, biometric authentication (e.g., fingerprint or face recognition), and full encryption to ensure the protection of company data. All security protocols must be strictly followed to safeguard against unauthorized access, data loss, or theft.

6. Social Media and Internet Access Standards

The use of social media and internet access during business hours should be governed by the following guidelines:

- **Social Media Policy:** Employees are prohibited from sharing confidential company information on personal or business social media channels without prior written approval from authorized personnel. Only designated individuals are authorized to post business-related content on official social media accounts, ensuring that all posts align with the organization's communication and security standards.
- **Work Email Usage:** Work email accounts are for professional use only. Personal use of work email is prohibited unless explicitly authorized by the organization, and even then, it should be limited to specific, non-work-related matters that do not interfere with business operations. Employees must avoid using work email for any activities that could potentially compromise the security or integrity of the organization.

- **Internet Use during Work Hours:** Employees must exercise discretion when using the internet during work hours. Access to non-work-related websites, online services, or social media should be strictly avoided unless such access is required for business-related tasks or research. Employees must remain focused on their work responsibilities to maintain productivity and reduce security risks associated with unmonitored internet use.
- **Monitoring Compliance:** The organization reserves the right to monitor internet usage and social media activity to ensure compliance with these policies and protect the company from potential security threats, data breaches, or inappropriate behavior. Monitoring activities will be conducted in a manner that respects employee privacy while safeguarding company assets and information.

7. AI Governance and Compliance

As Venturegamez continues to explore and incorporate Artificial Intelligence (AI) technologies to improve operational efficiency and innovation, the use of AI by employees and partners must be done in a manner that aligns with national and international standards and also with the company's values.

Venturegamez is committed to using AI systems that are free from bias. AI models must be regularly audited for fairness and to ensure they do not discriminate against individuals based on race, gender, age, or any other protected characteristic.

All decisions made by AI systems must have a level of human oversight to ensure accountability. AI should not be used to make decisions that could have significant negative impacts without human intervention or review.

Employees and partners must immediately report any misuse or security concerns related to AI technologies, including data breaches, model vulnerabilities, or unethical use, to the IT Department at Venturegamez.

In the event of an AI system failure or cybersecurity incident, the company's Business Continuity Plan (BCP) will include specific protocols for mitigating risks related to AI, including recovery of affected systems, data, and services.

8. Cybersecurity Policy Framework

All technology assets, including sensitive data, systems, applications, and networks, must be continuously monitored, secured, and safeguarded against potential cyberattacks. This includes implementing advanced security measures and regular vulnerability assessments to identify and address potential weaknesses before they can be exploited.

Employees shall be annually and thoroughly trained to identify and respond to a wide range of cybersecurity threats, including phishing, malware, social engineering, and other forms of cyberattacks. A clear reporting protocol must be established, ensuring that all potential security incidents are promptly communicated to the IT team for rapid assessment and mitigation.

9. Passwords

To ensure robust security at every level, the following password and authentication guidelines must be strictly adhered to:

- **Passphrase Strength:** Employees are required to use strong, complex passphrases consisting of a combination of upper/lowercase letters, numbers, and special characters for all systems accounts. Passphrases must avoid using easily guessable information, such as significant dates, names of relatives or pets, and telephone numbers.
- **Multi-Factor Authentication (MFA):** MFA must be implemented wherever feasible, providing an additional layer of security to protect sensitive information and systems.
- **Regular Passphrase Updates:** Passphrases must be updated at least every one hundred and eighty (180) days, and employees should use unique passphrases for each system to prevent the risk of cross-platform breaches.

10. Phishing Attempt

Given the prevalence of phishing and other email-based attacks, all employees must follow these best practices to ensure email security:

- **Attachment and Link Caution:** Do not open attachments or click on links from unknown or suspicious email addresses or sources. Always verify the sender's authenticity before interacting with email content.
- **Phishing and Spam Reporting:** Junk, spam, and phishing emails should be immediately flagged and reported to the IT department for further investigation and action.
- **Advanced Email Filtering:** Email filtering tools should be optimized and configured to automatically block known phishing attempts, malware, and other malicious content from reaching employees' inboxes.

If you receive an email that seems suspicious or if you have any doubts about the authenticity of the sender, please contact the IT department at Venturegamez for verification.

11. Risk Management

Venturegamez is steadfast in its commitment to proactively identifying, assessing, and mitigating information security risks to protect the organization's assets and data. This comprehensive risk management process includes:

- **Risk Assessments:** Risk assessments will be conducted regularly to identify, evaluate, and prioritize potential threats and vulnerabilities. These assessments will involve cross-functional teams to ensure all possible risks are considered, from cyber threats to physical security vulnerabilities.
- **Risk Mitigation:** Once risks are identified, immediate and appropriate measures will be taken to mitigate them. This includes the implementation of advanced security controls such as encryption, firewalls, intrusion detection systems, and strict security protocols to safeguard sensitive information and prevent unauthorized access.
- **Incident Documentation and Review:** All security incidents, breaches, and near-misses will be meticulously documented and analyzed to determine root causes, response effectiveness, and opportunities for improvement. This post-incident review process is vital for continually refining the organization's security strategy and strengthening its overall security posture.

12. Privacy and Data Protection

Venturegamez is committed to: (a) ensuring the confidentiality and integrity of sensitive personal and corporate data, both in transit and at rest; (b) implementing strong encryption mechanisms for storing and transmitting sensitive information; (c) limiting access to personal data to only those employees or contractors who need it to perform their job duties; (d) implementing regular audits and reviews to ensure compliance with data protection laws and organizational policies; and (e) ensuring the confidentiality and integrity of sensitive personal and corporate data, both in transit and at rest, through robust security measures.

Further information regarding the processing of employee and partner data can be found in Venturegamez's Privacy Policy.

13. Incident Management and Response

Venturegamez recognizes the importance on the swift identification and resolution of security incidents to ensure the protection of its systems and data. As part of this commitment, any security incident or breach, including data leaks, unauthorized access, malware infections, or any other form of compromise, must be reported immediately to the IT Department of the company.

Once an incident is reported, a comprehensive and well-defined incident response protocol is enacted. This protocol includes key steps such as containment, eradication of the threat, and recovery of affected systems and data. The goal is to quickly restore normal operations while minimizing the impact on the organization. This response process is designed to be flexible and adaptable to a variety of security events, ensuring that no matter the nature of the breach, the response remains effective, immediate and efficient.

Following the resolution of an incident, Venturegamez shall conduct a thorough post-incident review. This review aims to identify the root causes of the security breach and assess the effectiveness of the incident response. The findings from this analysis will be used to implement additional preventative measures, strengthen existing security protocols, and reduce the likelihood of similar incidents in the future.

14. Network and System Security

To protect the integrity of Venturegamez network and systems, firewalls and other advanced security measures will be implemented and configured to safeguard the network perimeter. These mechanisms will be implemented with the IT department's help and they are essential in preventing unauthorized access and defending against potential threats that could compromise the security of the network. In addition, to ensure robust security, all systems and software must be regularly updated with the latest security patches and fixes.

To maintain the company's security integrity, every device within the organization must have up-to-date anti-virus and anti-malware software installed. Therefore, it is essential that all employees adhere to update notifications and promptly implement these updates.

Furthermore, to ensure operational continuity and resilience, Venturegamez will maintain comprehensive Business Continuity Plans and Disaster Recovery Plans. These plans are designed to ensure the company can continue to operate during and after disruptive events, minimizing downtime and preserving data integrity. As part of our data protection strategy, critical data will also be backed up regularly, with secure copies stored off-site. This ensures that, in the event of data loss or system failure, we can quickly recover and resume operations without significant disruption.

15. Periodical Awareness and Training

A key component of Venturegamez security strategy is ensuring that all employees and partners are well-equipped to recognize and respond to potential threats. As such, mandatory information security awareness training will be required for all staff, both initially and on an ongoing basis, according to the needs of each team and the company's official training calendar.

In addition to formal training, which will cover essential security protocols, best practices, and the latest cybersecurity threats, periodic cybersecurity simulations, such as phishing exercises, will be conducted to assess and reinforce employee awareness and response capabilities. These simulations will serve as valuable tools in identifying potential vulnerabilities and ensuring that Venturegamez workforce remains vigilant in safeguarding company data and systems.

16. Monitoring, Auditing, and Enforcement

In order to uphold a high level of security and compliance, all Venturegamez systems will undergo continuous monitoring for signs of unusual activity, potential breaches, and non-compliance with the pre-established policies.

In addition to ongoing monitoring, routine audits will be carried out to evaluate compliance with this policy. These audits will help pinpoint areas where adherence may be lacking and offer opportunities for enhancing security practices and will include reviews of system logs, user behavior, and overall policy adherence, providing valuable insights to fortify security protocols and optimize operations.

To maintain the integrity of this policy, violations will be met with appropriate disciplinary measures. Depending on the gravity of the violation, consequences may include dismissal, legal proceedings, and/or financial penalties, always according to the civil and employment legislation.

17. Questions and Suggestions

For any questions, suggestions or concerns regarding this policy, please contact the IT department of Venturegamez via Jira Ticket and/or the compliance team at compliance@venturegameznl.com.

18. Policy Review and Updates

To ensure its continued relevance and effectiveness, this Information Security Policy will undergo annual review. Furthermore, Venturegamez will proactively update the policy in response to significant changes in technology, regulations, or company internal operations.

All employees, consultants, partners and relevant stakeholders will receive timely communication regarding any updates.

Version	1.0
Effective Date:	May 1 st . 2025
Last Review Date:	May 1 st , 2025