SimVenture

Venture Simulations Ltd (Trading as 'SimVenture')

Last updated: January 2026

Information Security Policy

Venture Simulations Ltd / VSL

Purpose

The purpose of an information security policy (ISP) is to provide a high-level framework defining how an organization protects its data and systems, ensuring Confidentiality, Integrity, and Availability (CIA) of information while meeting legal/regulatory needs and fostering a security-aware culture. It sets rules for access, defines responsibilities, manages risks, and guides responses to security incidents, ultimately safeguarding assets, reputation, and customer trust. Customer Personal Data: We are required by law to protect this information and any breaches are taken very seriously and could be extremely costly.

Malware Protection

- Users must ensure that anti-virus software, including a firewall (preferably Bitdefender), is installed and that all protection features are enabled.
- Users must run an anti-virus scan on their PC at least once per week.
- Users must not visit known malicious web sites if warned by the anti-malware product unless approved by the IT team.
- Users must not try to uninstall or disable anti-virus software without permission from the IT team. Any messages suggesting that antivirus protection has been disabled should be investigated immediately.

Device Security

- All PCs must be configured to run automatic updates for Windows or any other operating system in use.
- All application software must be kept up to date, and updates must be applied when prompted.
- PCs that are used outside the office must have encryption enabled on all storage drives.
- Sensitive data stored on USB drives must be handled carefully, and files must be deleted from the device once a transfer has been completed.

Access Controls

- All passwords must comply with the organisation's password guidelines.
- Two-factor authentication (2FA) must be enabled wherever possible.

- When working in public locations, users must take care when logging into any account to ensure that their credentials cannot be observed by others.

- User accounts must be granted only the privileges required for normal use, and administrative accounts must not be used by default.

Networking

- Users must ensure that a firewall (preferably Bitdefender), is installed and that all protection features are enabled.

- Open public Wi-Fi networks must be used with caution, and sensitive information must not be transmitted over such networks.

Email

- All emails should be scanned by anti-virus / anti-malware software. Email attachments must be scanned by an anti-virus product before delivery.

- All emails must be checked for phishing attempts in accordance with the organisation's guidance.

- Confidential information must only be stored on a PC when absolutely necessary and must be deleted once it is no longer required.

Data Disposal

- Sensitive information must only be retained for the minimum time needed to provide a reasonable level of service.

- Backups of data may be retained for up to a year.

Data Protection

- All Staff must work within the constraints of the company Data Protection policy.

- Users have the right to request that their personal data is removed from the system.

Bring Your Own Device (BYOD) Policy

All individuals who make use of BYOD must take responsibility for their own device and how they use it.

They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of company information (as well as their own information);

- Invoke the relevant security features for the device.

- Maintain the device themselves ensuring it is regularly patched and upgraded using updates provided by vendors.

Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data.
- Keep information confidential where appropriate.
- Maintain the integrity of data and information and take responsibility for any software they download onto their device.
- Use access controls consistent with this policy.
- Ensure that software on personally owned devices are appropriately licenced.
- Encrypt sensitive documents or devices as necessary.

Data Breach and Incident Response

- All security incidents and / or data breaches must be reported to the CTO immediately.
- The company management team will meet as soon as possible to formulate a plan and agree any response.

Password Guidelines

- Passwords should have a minimum of 8 characters, ideally with a mix of letters, numbers and control characters
- Users should ideally use strong passwords of randomised characters (as suggested by Google password manager).
- If a password contains recognizable words, it should have a least 2 unconnected words and not use common phrases that could be easily guessed.
- Passwords should not contain information that could be gleaned from your online profile – e.g. Pet's names, significant dates, etc.
- Passwords must not be reused for different accounts.
- Passwords must not be shared.
- Passwords should be significantly different to other passwords already in use.

How to check for Phishing Emails

Assess all emails to check for Phishing.

Red flags are:

- Lack of personalization – your name, account number, etc is not used in the email

- A request for you to follow a link to enter information, especially asking you to login to an account.

- Any unusual request from a trusted person, especially involving sensitive information or money.

- Any request asking you to act urgently.

- Spelling mistakes or poor English in the text of the email.

- Attachments with the email that you have not specifically asked for.

If you suspect an email might be phishing, check the following:

- The return address of the email – is this consistent with the supposed sender? Is the domain correct? It might be deliberately misspelled (e.g. an extra letter) so check carefully.

- The address of any link in the email. If you hover over the link then the email client should show you the address. If this looks in any way unusual then be very careful.

- If in any doubt, do not respond and inform the IT team. Contact the supposed sender by phone or another non-email method to confirm whether they did actually send the email.

- If after these check you are suspicious, do not open any attachments or click on any links.