VISIVE®

POWERED BY SMART TECHNOLOGY

IT Security Policy

Version 1.1 December, 2021

Contents

1. Purpose

The policy provides a framework for a standard Visive Group Ltd (Visive) procedure to ensure the physical and data security of all portable devices.

2. Scope

This policy applies to all Visive employees. Employees are responsible for ensuring that they follow the procedures outlined in this policy. Any queries on the application or interpretation of this policy must be discussed with a Visive Director prior to any action being taken.

3. Hardware and software

The organisation provides hardware and software which is compatible with all Visive systems. All appropriate hardware and software is procured and installed by the Technical and Operations Director, and users must not install additional hardware or software without first seeking consent from the Technical and Operations Director. Non-Visive provided portable devices should not be connected to Visive's data Network without prior permission.

Software downloaded from the Internet must not be loaded onto systems managed and supported by the Technical & Operations Director. Software obtained illegally must not be loaded onto the portable device.

4. Protection of portable hardware

Where the Company issues a portable device to an employee, security of the device is the responsibility of the user at all times, and the following must be adhered to:

- When not in use, portable devices should be kept in a secure location such as a locked drawer
- While in transit, portable devices should be in a suitable carrying case and should be kept out of view wherever possible
- Portable devices should not be left unattended in a public place, and should not be left in an unattended vehicle
- Password details should not be kept in the same location as the portable device
- Portable device should not be left within sight of ground floor windows or within easy access of external doors

The Company reserves the right to make a payroll deduction to cover the cost of portable hardware which is lost or damaged due to an employee's negligence.

5. Security of data

Confidential data must only be installed on portable devices which have been supplied by the external provider and have an appropriate level of access security/ encryption implemented. Where this is required a Director must be informed in advance of the portable devices use.

Each Visive portable device must be accompanied by a Portable Device Deployment Form and shall require a user signature to indicate acceptance. Completed copies of the form will be retained by Visive.

If work is being carried out in public places, meeting rooms and other unprotected areas, care should be taken to avoid the un-authorised access to and or disclosure of the information stored and processed by the portable device.

Care should be taken by the staff using the portable device to minimise the risk of unauthorised persons overlooking the screen.

Confidentiality Policies apply equally to information whether in the office or at home. Failure to maintain confidentiality may result in a disciplinary action.

Data backup solution is provided centrally on Visive data network and not on each portable device. ***It is the user's responsibility to ensure that their data is frequently copied to the data network, for backup purposes***.

6. Virus control

All portable devices have Anti-Virus software installed by the external provider. This package is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files. Users must not alter the configuration of this package.

The anti-virus system's database of virus definitions must be upgraded on a regular basis; daily if possible. All portable devices must be connected to the network in order for virus updates to be applied.

7. Password security

Passwords must not be shared; and must not be easily recognisable e.g. date of birth, name of partner, or simple numbers such 111111. A mixture of numbers, letters and special characters should be used.

Passwords need to be changed regularly to ensure security of data.

8. Internet / email

The Internet, Email, and Social Media Policies of Visive are equally applicable to portable devices.

9. Losses and confidentiality / security breaches

Incidents that constitute a loss of hardware or data, which could potentially lead to a breach of confidentiality, need to be reported immediately. Please note disciplinary action may also be taken against you in line with Company's Disciplinary Policy, where it is discovered you did not take proper care of equipment issued to you. The Company can also exercise its right to recover any costs that it occurs from you.

10. Accounting / audit

The software and information held on portable devices are subject to the same audit procedures as Visive computer systems. This also covers information and data stored on removable media e.g. floppy disks, memory sticks. The Company reserve the right to recall portable devices at any time to audit their use.

11. Travel and business expenses

Users of portable devices must comply with current legislation regarding the use and retention of client information and use of computer systems. These include, but are not limited to:

- The Data Protection Act 1998
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990

12. Termination of employment

Upon termination of employment or contract, the user is required to return all Visive owned properties on or before the last day of employment.

13. Breach of IT security policy

All employees are required to adhere to this policy. Employees should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example a breach of confidentiality or activity causing serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal.

14. Document control

Issue No.	Date	Reason	Updated by
1.0	24/08/2017	Policy creation	C Tweed