**Videcom Security Limited.**
**Fordoun House, Rue De St Lawrence, Waltham Abbey, Essex, EN9 1PF.**
**Tel: +44 1 992 714604**
**Email: sales@videcomsecurity.co.uk Web: videcomsecurity.co.uk**

# Videcom Security Ltd
# Acceptable Usage Policy
# Computers, Telephones, Mobiles and IT Equipment

This Acceptable Usage Policy covers the security and use of all Videcom Security Ltd and their customers' information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Videcom Security Ltd employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Videcom Security Ltd business activities worldwide, and to all information handled by Videcom Security Ltd relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Videcom Security Ltd or on its behalf.

**Computer Access Control – Individual's Responsibility**

Access to the Videcom Security Ltd IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Videcom Security Ltd IT systems.

**Individuals must not:**

- Allow anyone else to use their user ID/token and password on any Videcom Security IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Videcom Security Ltd IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Videcom Security Ltd IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Videcom Security authorised device to the Videcom Security network or IT systems.
- Store Videcom Security data on any non-authorised Videcom Security equipment.
- Give or transfer Videcom Security data or software to any person or organisation outside Videcom Security without the authority of Videcom Security.

Give any engineer/admin Access Passwords to end users, customers or other individuals without proper permission and documentation. Customer accounts including those used for admin purpose must be set up individually. This also applies to remote access systems such as TeamViewer where individual Customer Access Passwords will issues as additional site users.

**Internet and email Conditions of Use**

Use of Videcom Security internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Videcom Security in any way, not in breach of any term and condition of employment and does not place the individual or Videcom Security in breach of statutory or other legal obligations.

**All individuals are accountable for their actions on the internet and email systems.**

Individuals must not:

• Use the internet or email for the purposes of harassment or abuse.
• Use profanity, obscenities, or derogatory remarks in communications.
• Access, download, send or receive any data (including images), which Videcom Security considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
• Use the internet or email to make personal gains or conduct a personal business.
• Use the internet or email to gamble.
• Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
• Place any information on the Internet that relates to Videcom Security , alter any information about it, or express any opinion about Videcom Security , unless they are specifically authorised to do this.
• Send unprotected sensitive or confidential information externally.
• Forward Videcom Security mail to personal (non-Videcom) email accounts (for example a personal Hotmail account).
• Make official commitments through the internet or email on behalf of Videcom Security unless authorised to do so.
• Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
• In any way infringe any copyright, database rights, trademarks or other intellectual property.
• Download any software from the internet, allow third party access to your computer or install any software without prior approval. Approval can only be made by Bill Mead MD, Nick Burridge Cedar Tree Systems.
• Connect Videcom Security devices to the internet using non-standard connections.

**Clear Desk and Clear Screen Policy**

In order to reduce the risk of unauthorised access or loss of information, Videcom Security enforces a clear desk and screen policy as follows:
• Personal or confidential business information must be protected using security features provided for example secure print on printers.
• Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
• Care must be taken to not leave confidential material on printers or photocopiers.
• All business-related printed matter must be disposed of using confidential waste bins or shredders.

**Working Off-site**

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:
• Working away from the office must be in line with Videcom Security remote working policy.
• Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
• Laptops must be carried as hand luggage when travelling.
• Information should be protected against loss or compromise when working remotely (for example at home or in public places).

• Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

**Mobile Storage Devices**

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Videcom Security authorised mobile storage devices with encryption enabled must be used , when transferring sensitive or confidential data.

**Software**

Employees must use only software that is authorised by Videcom Security on Videcom Security Ltd computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Videcom Security computers must be approved and installed by the Videcom Security IT department. If in Doubt, ask.

**Individuals must not:**

Store personal files such as music, video, photographs or games on Videcom Security IT equipment.

**Viruses**

The IT department has implemented centralised, automated virus detection and virus software updates within the Videcom Security Network.
All PCs have as minimum Windows antivirus software installed to detect and remove any virus automatically.

**Individuals must not:**

• Remove or disable any anti-virus software.
• Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Videcom Security anti-virus software and procedures.
• Accept advice or carry out any instruction from third party agents either by telephone or email regarding any infection or issue on their Videcom IT/Telephone equipment without prior permission.

**Telephony (Voice) Equipment Conditions of Use**

Within reason: Use of Videcom Security voice equipment is intended for business use. Individuals must not use Videcom Security Ltd voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

**Individuals must not:**
• Use Videcom Security Ltd voice for conducting any private business.
• Make hoax or threatening calls to internal or external destinations.
• Accept reverse charge calls from domestic or International operators, unless it is for business use.

**Actions upon Termination of Contract**

All Videcom Security equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Videcom Security at termination of contract. All Videcom Security data or intellectual property developed or gained during the period of employment remains the property of Videcom Security and must not be retained beyond termination or reused for any other purpose.

**Monitoring and Filtering**

All data that is created and stored on Videcom Security computers and mobile devices is the property of Videcom Security and there is no official provision for individual data privacy, however wherever possible Videcom Security will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Videcom Security has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

**This policy must be read in conjunction with:**

- Computer Misuse Act 1990
- Data Protection Act 1998

It is your responsibility to report suspected breaches of security policy without delay to your line management, or a company Director.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Videcom Security terms and conditions of employment.

Security of our and the security of our customers data must be taken seriously and is an important part of our daily business activities. The Videcom acceptable data usage policy extends to customer sites where we operate and also relates to third party data, customer computers and customer computer networks we may have access to while working on customer premises, our customers may also have their own data and fair usage policies in which case these policies may take precedent to any Videcom Security Policy.

All employees are required to confirm they have read and accepted the Videcom Usage Policy, a copy of which is available on request; a copy of this acceptance will be retained on individual staff files.