CVC-HR-PO-002

Information Security & Data Protection Policy

Date	Description	Name	Position
26/02/2019	Policy	Shane Davies	Managing Director
03/03/2022	Annual Review	Michael Vincent	Managing Director
03/07/2023	Annual Review - Document Updated and new IT provider details added	Chris Wilson	Chairman
10/07/2023	Document Format Updated	Sophie Kirk-Ash	HSEQ

POLICY STATEMENT

ClearView Communications Ltd, which provides the design, installation and maintenance of fire and security systems, is committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets.

The purpose of this document is to define the role that ClearView Communications Ltd's Board of Directors takes in ensuring commitment to information security & Data Protection, the development and propagation of this policy, and the assignment of appropriate roles, responsibilities and authorities to protect ClearView Communications Ltd's assets from all relevant threats, whether internal or external, deliberate or accidental.

INFORMATION SECURITY & DATA PROTECTION POLICY

AIMS:

1. Ensure compliance with all applicable laws regarding data protection, information security, and compliance monitoring.
2. Protect the Company, our employees and our customers from the risk of financial loss, harm, loss of reputation, or libel.

OBJECTIVES & Principles:

1. Support core business functions and providing evidence of conduct and the appropriate maintenance of associated tools, resources and outputs to clients and third parties.
2. Meet legislative, statutory and regulatory requirements.
3. Deliver services to staff and stakeholders in a consistent and equitable manner.
4. Provide continuity in the event of a disaster.
5. Protect the interests of the organisation and the rights of employees, clients and present and future stakeholders.
6. Ensure that the Company conducts itself in an orderly, efficient and accountable manner.
7. Ensure the safe and secure disposal of confidential data and information assets.
8. Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each body's rules or terms.
9. Ensure that no document is retained for longer than is legally or contractually allowed.
10. Mitigate against risks or breaches in relation to confidential information.

SCOPE:

The policy also applies to all individuals that use or operate within our IT systems, including networks, laptops, desktops, telephones, tablets or any other facility that is provided for communication purposes.

ROLES & RESPONSIBILITIES:
The Board of Directors are responsible for setting and approving the Information Security & date protection policy. All employees and staff are responsible for adhering to the requirements of the policy and fulfilling any duties relation to assigned roles, responsibilities or authorities. The consequences for breaching the policy are set out in ClearView Communications Employee Handbook.

DATA PROTECTION OFFICER:
Chris Wilson (Chairman)
ClearView Communications Ltd
Chris.wilson@clearview-communications.com

Relevant third parties associated with ClearView Communications Ltd's IT and network management:

Role	Contact Company
Telephony services & maintenance	Cloud Voice & Data (The Old Wagon Factory, 11a Blatchington Road, Seaford, BN25 2AB)
IT services & maintenance	Fusion Technology Limited (Rivermead House, Bishop Hall Lane, Chelmsford, CM1 1RP)
Firewall services & maintenance	Crystaline Communications, Boston House Business Centre, 69-75 Boston Manor Road, Brentford, TW8 9JJ

1. User Access

1.1 User Account Creation and Authorisation Process

1.1.1 User accounts are created based on verified business needs and approved by the relevant line manager or authorised personnel.

1.1.2 Access to specific applications, systems, or data is granted based on the principle of least privilege, ensuring users have only the necessary access rights to perform their job responsibilities.

1.1.3 User access authorization requests are documented and maintained for auditing purposes.

1.1.4 User access is promptly revoked or modified upon termination, resignation, or role changes within the organisation.

1.1.5 HR and IT departments collaborate to ensure terminated employees' access is deactivated immediately to prevent unauthorised access to systems or data.

2. Review of Data

2.1.1 User access rights are reviewed periodically to ensure they align with current job responsibilities, business requirements and legal requirements.

2.1.2 Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, the Company will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices.

3. Removal of Data & Retention

3.1.1 Line Managers promptly notify the IT department about any role changes or transfers to adjust access rights accordingly.

3.1.2 If the Company is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our firm, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

3.1.3 Once a record or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

3.1.4 The Company is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

3.1.5 Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support.

3.1.6 Where correspondence or memoranda that do not pertain to any documents having already be assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases or at a maximum, 2 years.

3.1.7 In accordance with GDPR requirements and Schedule 1 Part 4 of The Data Protection Bill, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.

3.1.8 Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our retention register schedule.

4. Erasure of Data

4.1.1 In specific circumstances, data subjects' have the right to request that their personal data is erased, however the Company recognise that this is not an absolute 'right to be forgotten'.

4.1.2 Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed

4.1.3 When the individual withdraws consent

4.1.4 When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
4.1.5 The personal data was unlawfully processed
4.1.6 The personal data must be erased in order to comply with a legal obligation
4.1.7 The personal data is processed in relation to the offer of information society services to a child
4.1.8 If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

5. Document Classifications

5.1 Public

5.1.1 (Everyone has access) - information that is freely obtained from the public and as such, is not classified as being personal or confidential.
5.1.2 Examples may include: public directory information, business registration information, social media posts, government publications)

5.2 Internal

5.2.1 (All employees have access) - information that is solely for internal use and does not process external information or permit external access.
5.2.2 Examples may include: internal email communications, policies, processes, memos.

5.3 Restricted

5.3.1 (Most employees have access) – information that is sensitive and requires restricted access to specific groups dependent upon job role.
5.3.2 Examples may include: contract data, customer asset data and records)

5.4 Confidential

5.4.1 (Directors / HR) - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication
5.4.2 Examples may include: non-disclosure agreements, personal employee information, legal documents.

6. Acceptable Use

6.1 Compliance with Laws and Regulations

6.1.1 Users must adhere to all applicable laws, regulations, contractual obligations governing information security, data protection and intellectual property rights.

6.2 Hardware & Software

6.2.1 Ensure you only use hardware that has been set up by our IT provider with the correct anti-virus and security software.
6.2.2 Employees should not download or install software from untrusted sources without prior authorisation from the IT provider and Line Manager

6.2.3 Report any stolen or damaged equipment to your line manager immediately.

6.3 Device Security

6.3.1 Ensure you log off or lock your device when not in use.

6.3.2 Do not leave your workstations, laptops, or mobile phones unattended in public spaces.

6.4 Data Storage and Confidentiality

6.4.1 All files must be stored on the network drive, which is backed up regularly to avoid loss of information.

6.4.2 Confidential documents should not be left unattended or exposed to unauthorised individuals.

6.5 Information Transfer

6.5.1 Avoid transferring sensitive information to other devices unless necessary. When mass transfer of such data is needed, request assistance from our IT provider to do this securely.

6.5.2 Ensure the person you are sending the data to has the authorisation to read/receive it.

7. Internet

7.1.1 Avoid accessing or visiting websites that contain offensive, illegal, or inappropriate content.

7.1.2 Exercise caution when clicking on links or downloading files from the internet to prevent the risk of malware, viruses, or other security threats.

7.1.3 Ensure that you are not infringing any copyright by downloading, copying, distributing material from other entities.

7.1.4 When purchasing goods online do not disclose credit card details unless you are confident that the site is trustworthy and reliable.

8. Email

following guidelines outline acceptable email use:

8.1.1 Use company email accounts only for business-related purposes.

8.1.2 Do not use company email accounts to send or receive personal emails or access personal email accounts or private business accounts except as permitted by company policies.

8.1.3 Always consider the most appropriate method of communication and remember that the security and confidentiality of email is not guaranteed when transmitting confidential data.

8.1.4 Exercise caution when sending emails containing sensitive or confidential information. Ensure that recipients are authorised to receive such information.

8.1.5 Avoid including sensitive information, such as account credentials or personal identification details, in the body of an email.

8.1.6 Only send attachments that are necessary for business purposes and ensure they comply with company policies and guidelines.
8.1.7 Use professional language, tone, and grammar when composing emails.
8.1.8 Avoid using email to engage in disrespectful, offensive, or discriminatory language or behaviour.
8.1.9 Do not open attachments from unknown or suspicious sources.
8.1.10 Be aware of social engineering techniques used to deceive individuals into divulging sensitive information. Verify the authenticity of email requests before responding or taking any action.
8.1.11 Good housekeeping procedures should be undertaken to ensure that stored data is not stored for longer than necessary.
8.1.12 Report any suspected or actual security incidents related to email, such as unauthorised access, email spoofing, or phishing attempts, to the IT department immediately.
8.1.13 Avoid transferring sensitive information to other devices unless necessary. When mass transfer of such data is needed, request assistance from our IT provider to do this securely.
8.1.14 ClearView Communications Ltd reserves the right to monitor and audit the use of company information assets, systems, and resources to ensure compliance with this Acceptable Use policy. Non-compliance with this policy may result in disciplinary action.

8.2 Storage of emails

8.2.1 Employees should ensure they regularly audit their emails in order to archive or delete those that contain information that is no longer required in order for ClearView Communications Ltd to comply with its obligations under current data protection legislation.

8.3 Unauthorised use of email and internet

8.3.1 Any messages that could constitute bullying, harassment or other detriment.
8.3.2 Accessing social networking sites using Company equipment or during work time unless this is necessary for the completion of business-related tasks (e.g., Marketing)
8.3.3 On-line gambling
8.3.4 Accessing or transmitting pornography
8.3.5 Accessing other offensive, obscene or otherwise unacceptable material
8.3.6 Transmitting copyright information and/or any software available to the user
8.3.7 Posting confidential information about other employees, the Company or its customers or suppliers.

9. Data Breach

9.1.1 ClearView Communications Ltd utilises a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome.
9.1.2 In cases of data breaches, the Data Protection Officer (DPO) is responsible for carrying out a full investigation, appointing the relevant

staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

9.1.3 A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and record purposes.

9.1.4 Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee held.

9.1.5 A review of the procedure associated with the breach is conducted to determine root cause analysis and training requirements.

10. Bring Your Own Device (BYOD)

10.1.1 Any device that has not been approved by the I.T. Department will not be permitted access to our network. Any personal device that has not been checked and approved for use by a member of the I.T. team will be unable to connect to ClearView Communications Ltd's network.

10.1.2 Any Company data and confidential information available on a personal device should be accessed by the authorised user only and this should be in line with the existing IT and data protection policies. No access to the device or Company's network will be permitted for third party users.

10.2 Usage of your own device for business purposes:

10.2.1 personal devices remain the responsibility of the employee and all associated costs for the device and the running of the device shall remain with the employee.

10.2.2 ClearView Communications Ltd accepts no responsibility for any loss or damage to personal devices that are the result of employee failure to observe rules, procedures or instruction, or, as a result of your negligent behaviour

10.2.3 Misuse of Company information, data and/or software provided by ClearView Communications Ltd will be treated as gross misconduct which will result in formal disciplinary action being taken up to and including dismissal.

10.2.4 Upon termination of employment, you must ensure that all Company data and software is removed from your device on your last day of work at the latest. Evidence of this must be presented to the IT department, who may require you to submit your device to them for inspection and removal of company data/software if necessary.

11. Company Issued Mobile Phones

11.1.1 Only certain job roles require the provision of a Company mobile phone. Where provided, they are for business use only.

11.1.2 Employees should ensure they keep their company issued mobile phone in good working order. The mobile phone should remain charged and connected to the network (as far as coverage permits) during working hours so business calls can be received as necessary.

11.1.3 When visiting clients/customers or carrying out work on other Company site, you may be required to turn off your Company mobile phone. Employees must observe any site-specific requirements and ensure they comply with them.

11.1.4 The cost of line rental and normal business call usage will be covered by ClearView Communications Ltd.

11.2 Inappropriate Use

11.2.1 Monitoring of the use of Company mobile phones is carried out by the company, in line with ClearView Communications Ltd's monitoring policy. All data processing undertaken by monitoring in this way will be done in accordance with the General Data Protection Regulation and Data Protection Act. Abuse of ClearView Communications Ltd mobile phones may result in disciplinary action.

11.2.2 Unless permitted by an employee's contract of employment, personal calls should not be made using the Company mobile. ClearView Communications Ltd reserves the right to make a deduction from an employee's next salary payment of the cost of any personal phone calls made. Employees may suggest an alternative arrangement for repayment of this, to be discussed and agreed with the employee's line manager.

11.2.3 Any messages sent by text, or any answerphone messages left on voicemail services should comply with the usual business standards surrounding correspondence sent and comply with the usual conventions and best practice surrounding business communications. Disciplinary action may be taken when an employee sends an inappropriate text or makes an inappropriate voicemail message.

11.2.4 Any obscene or offensive communications, or defamatory or malicious communications, may result in disciplinary action. ClearView Communications Ltd is likely to view this kind of communication as gross misconduct which could result in immediate dismissal. Any inappropriate, offensive or obscene communications received by an employee on their Company mobile phone should be reported to their line manager.

12. Loss or damage of Company Equipment

12.1.1 Employees are responsible for the safekeeping of their Company issued equipment (Laptops, Mobiles, Tablets etc). Any loss or damage caused by the employee's negligence will result in a charge for the repair or replacement. ClearView Communications Ltd reserves the right to make a deduction from an employee's next salary payment for the cost of repairs or replacement. Employees may suggest an

alternative arrangement for repayment of this, to be discussed and agreed with the employee's line manager.

12.1.2 Company mobile phones should be secured with a password or PIN and kept out of sight. Company mobile phones must not be left in a Company vehicle.

12.1.3 Reasonable precautions should be taken by employees to limit the risk of their Company mobile phone being stolen. If it is stolen, employees should inform their line manager immediately.

13. Return of equipment

13.1.1 Employees may be requested to return their Company equipment at any time. Employees must return their device upon termination of their employment. Whenever returned, the Company mobile phone must be accompanied by any additional accessories that were also issued to the employee.

13.1.2 ClearView Communications Ltd reserves the right to make a deduction from an employee's final salary payment of the cost of the replacement of the phone and/or any missing accessories, if any of these are missing or damaged. Employees may suggest an alternative arrangement for repayment of this, to be discussed and agreed with the employee's line manager.

13.1.3 ClearView Communications Ltd reserves the right to remove the Company device from an employee should any terms of this policy be breached. Inappropriate use of the telephony infrastructure or mobile phones may be treated as gross misconduct and could result in summary termination of employment.

14. Password Management

14.1.1 In order to maintain the confidentiality of information held on or transferred via the Company's Facilities, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Company's network and to our financial, HR and CRM systems.

14.1.2 Your password must be changed upon first log on

14.1.3 Passwords must be strong with a mix of upper case, lower case, numerical and symbols.

14.1.4 Passwords must be kept confidential and not shared.

14.1.5 Where possible you must use two factor authentication

14.1.6 Passwords should be changed periodically and immediately upon a compromise or breach.

14.1.7 Despite the use of a password, the Company reserves the right to override passwords and obtain access to any part of the network or system that is required. Audit trails are also kept for the purpose of identifying and investigating any potential or actual breach in security.

15. Network Access Controls

15.1.1 All firewalls are tracked and documented within the management portal “Meraki”. Access to this portal is restricted to our firewall maintenance provider and IT provider.

15.1.2 Clearview segments business operations into separate virtual networks, currently Corporate, Corporate Wireless and Guest. All inter-network communications are routed via the firewall, which blocks inter-network traffic by default.

15.1.3 By default, all inbound services are blocked at the network edge. Certain services are permitted to internal systems, based on a considered business justification and documented in the relevant system documentation.

16. Building Security

To enhance the security and confidentiality of confidential and sensitive data within the building, we have implemented the following measures:

16.1 Access Control and ID Cards

16.1.1 All employees, contractors, and authorised personnel are required to always possess and display a valid identification (ID) card while on the premises. This is also used as the employee’s access control card to allow access to the building. ID cards must be visibly worn and easily accessible for identification purposes. Unauthorised individuals or those without proper identification will be denied entry to the premises.

16.1.2 Employees must report lost or stolen ID cards to their Line Manager and HR immediately.

16.2 Visitor Management

16.2.1 Host employees are responsible for escorting their visitors throughout the building and ensuring they adhere to the organisation's policies and guidelines.

16.3 Access Monitoring

16.3.1 Surveillance cameras and access control systems are installed throughout the building to monitor entry points, common areas, and sensitive areas.

16.4 Restricted Areas

16.4.1 Certain areas or storage locations within the building may have restricted access due to the presence of confidential or sensitive information.

16.4.2 Access to these areas is limited to authorised personnel only, who must use their ID cards for entry. Unauthorised access or attempts to gain access to restricted areas should be immediately reported to your line manager or a Director.

17. Clear Desk Policy

17.1.1 All sensitive and confidential paperwork must be removed from the desk and stored in locked drawers or filing cabinets.
17.1.2 Any wastepaper containing sensitive or confidential information should be disposed of within the confidential wastepaper bins for secure disposal. Under no circumstances should this information be disposed of in regular wastepaper bins.
17.1.3 Computer workstations must be locked when the desk is unoccupied.
17.1.4 At the end of the workday, workstations should be completely shut down to ensure data security.
17.1.5 Laptops, tablets, and other hardware devices should be removed from the desk and stored in locked drawers or filing cabinets when not in use.
17.1.6 Keys for accessing drawers or filing cabinets should not be left unattended at the desk.
17.1.7 Printers should be treated with the same care as computer workstations under the Clear Desk Policy.
17.1.8 Print jobs containing sensitive and confidential information should be retrieved immediately.
17.1.9 Any remaining paperwork at the end of the workday should be properly disposed of or securely stored in the lockers following appropriate protocols.

18. Incident Reporting and Response

When an incident is suspected or observed, employees should follow these steps to report it:

18.1.1 Notify Line Manager: Immediately inform your line manager about the incident. Provide a clear and concise description of the incident, including any relevant details, such as the date, time, location, and individuals involved or affected.
18.1.2 Notify IT Provider: Simultaneously, report the incident to our IT provider, whose contact details are documented within this policy. They will assess the situation and initiate the appropriate response measures.

18.2 Line Manager Responsibilities

18.2.1 Upon receiving an incident report, the line manager is responsible for assessing the severity and potential impact of the incident.
18.2.2 If necessary, the line manager will escalate the incident to a Director for further action.
18.2.3 The line manager will coordinate with the IT provider, HR and any other relevant stakeholders to ensure a swift and effective response to the incident.

18.2.4 Throughout the incident response process, the line manager will maintain open communication with the affected employees, providing updates on the progress and outcome of the investigation.

18.3 IT Provider Responsibilities

18.3.1 The IT provider will promptly acknowledge receipt of the incident report and initiate appropriate measures to investigate and contain the incident.

18.3.2 They will work closely with the line manager and other relevant stakeholders to gather necessary information, perform forensic analysis if required, and identify the root cause of the incident.

18.3.3 The IT provider will coordinate with the necessary parties to mitigate the impact of the incident, restore affected systems or services, and implement measures to prevent future occurrences.

18.3.4 Throughout the incident response process, the IT provider will keep the line manager informed of the progress, findings, and actions taken.

Signed:

Name: Chris Wilson
Position: Chairman
Date: 10/07/2023