CYBER SECURITY POLICY

1. Introduction

1.1 This policy document does not form part of the terms and conditions of employment for employees at [Insert Organisation name], ("the Organisation").

1.2 This policy should be read in conjunction with the Organisation's Data Protection and Communications Policies. Where a conflict arises between this policy and the aforementioned policies – the aforementioned policies will prevail.

1.3 If you have any questions regarding these guidelines and how they apply to you, please consult [Insert manager's name] – your manager before taking any action that may breach these guidelines.

2. Implementation

2.1 This policy is intended to be a practical policy for everyday use within and outside the workplace. The measures outlined in this policy will help to protect your devices and data.

2.2 The Organisation will provide full training on the use of the measures detailed in this policy and will meet the full costs of implementing and maintaining such measures.

2.3 Once full training has been provided, any failure to follow any implemented measures detailed in this policy may, in serious cases, result in disciplinary action.

3. Physical Security

3.1 All equipment (phones, computers, tablets) should be password protected. Where possible biometric security should also be used, whether fingerprint or face recognition. All devices should be set to lock after a period of inactivity. This period of inactivity should be set to between two and five minutes, with five minutes being the maximum.

3.2 All devices should be transported in suitable cases or bags.

3.3 Devices should never be left unattended when in a public place or left in a parked vehicle. Care should be taken during airport security checks; your devices should remain in your sight wherever possible. Furthermore, you should not leave devices at hotel concierge desks, coat checks, cloakrooms, or anywhere – where they could be claimed accidentally or deliberately by another person.

3.4 In the case of bags, it is recommended that you leave a business card within your bag if you are separated from your bag – this will make reuniting you with your bag potentially easier.

4. Virtual Private Network (VPN)

4.1 Whenever away from your office, whether travelling or working from home, you should always use a Virtual Private Network (VPN) to ensure that your Internet access and email are secure. A VPN creates a secure private connection when accessing the Internet, email or other services while using a public network connection, such as a public WIFI connection.

4.2 All employees (and contractors, where applicable) should use a reputable, paid-for VPN service, such as NordVPN. A subscription will be provided to all employees. For contractors, a VPN subscription is a billable expense paid for by the Organisation for the period that the contractor provides services to the Organisation.

5. Public WIFI

5.1 All public WIFI connections or WIFI connections provided by another organisation can be used but should always be used in conjunction with your VPN.

5.2 Before connecting to a public WIFI, you should always confirm with the location providing the WIFI, the correct WIFI connection to use and the password. You should not assume that you will be automatically connected to the correct WIFI or that the WIFI appearing in your list of possible connections is the correct one, particularly if the names of the different WIFI connections look similar. This is to ensure that you connect to the correct WIFI and not another posing as the correct connection. This precaution is to avoid logging into a so-called "evil twin" WIFI connection that a malicious party deliberately sets up in order to harvest your log in details, card details or any other private information that you may send over a WIFI connection. This type of attack can also be used to persuade you to download malware, posing as legitimate software in order for the WIFI connection to work. This scam has previously been used in hotels, train stations and coffee shops.

Sample document – the remaining are clause headings only
Full document contains all clauses

6. Software Updates

7. Passwords

8. Two-Factor Authentication (2FA)

9. Sim Card Security

10. Organisation Devices

11 Social Media

12. Voice Cloning

13. Known Threat Methods & Scenarios

- Email phishing
- Spear phishing
- Emergency emails
- Emergency holiday emails
- HMRC or Gov emails
- Compromised email accounts – Business Email Compromise (BEC)
- Voice cloning

14. Duty to Report

15. Date of Implementation

16. Questions

17. Alteration of this Policy