Cyber and Data Security Policy

We are committed to ensuring the highest standards of cyber and data security to protect the confidentiality, integrity, and availability of all client information. Our approach includes the following measures:

1. **Data Encryption:** All sensitive data is encrypted both in transit and at rest using industry-standard encryption protocols.
2. **Access Control:** Strict access control measures are in place to ensure that only authorised personnel have access to client data. This includes the use of strong passwords, multi-factor authentication, and regular access reviews.
3. **Secure Communication:** All communications, including emails and file transfers, are conducted through secure, encrypted channels to prevent unauthorised interception.
4. **Regular Updates and Patching:** All software and systems are regularly updated and patched to protect against known vulnerabilities and security threats.
5. **Data Minimisation and Retention:** Only the minimum necessary amount of client data is collected and stored. Data is retained only for as long as necessary to fulfil the agreed-upon consulting services, after which it is securely deleted or anonymised.
6. **Awareness:** Ongoing awareness programs are conducted to ensure that (company name) stay informed about the latest cyber security threats and best practices.
7. **Confidentiality Agreements:** Non-disclosure agreements (NDAs) are signed with all clients (where relevant) to ensure confidentiality and trust in all consulting engagements.

By implementing these robust security measures, we strive to safeguard client data and maintain the highest level of trust and integrity in our consulting services.

Your name – Director

Mobile xxxxx

Aug 2024