Security Policy for bvda.co.uk

1. Purpose

The purpose of this policy is to establish and enforce a framework for ensuring the security of **bvda.co.uk**'s digital and physical assets. This policy aims to safeguard confidential information, prevent unauthorized access, and ensure the integrity and availability of our systems and services.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and users who interact with **bvda.co.uk**'s systems, services, and data. It covers all digital assets, devices, networks, and operations under the organization's control.

3. Data Protection and Privacy

- **Confidentiality**: All sensitive information (including personally identifiable information, financial data, and proprietary business data) will be encrypted both in transit and at rest, using industry-standard encryption protocols.
- **Privacy Compliance**: **bvda.co.uk** is committed to complying with data protection laws including the General Data Protection Regulation (GDPR), the UK Data Protection Act, and any applicable local laws regarding the processing and storage of personal data.
- **Data Retention**: Personal and sensitive data will only be retained as necessary to fulfill business and legal obligations and will be securely deleted when no longer required.

4. Access Control

- **Authentication**: All users must authenticate through multi-factor authentication (MFA) before accessing sensitive data or systems.
- **Authorization**: Access to data, systems, and resources is granted based on job roles, adhering to the principle of least privilege. Employees, contractors, and third parties will only have access to the resources they need to perform their roles.
- **Password Management**: Strong password policies will be enforced across all systems, requiring a minimum of 12 characters, including a mix of letters, numbers, and special characters. Passwords must be changed regularly, and the reuse of passwords will be prohibited.

5. Security Monitoring and Incident Response

- **Log Management**: All systems will generate logs of access events, administrative actions, and security-related activities, which will be reviewed regularly for suspicious activities.
- **Intrusion Detection**: An Intrusion Detection System (IDS) will monitor network traffic for potential malicious activities, including unauthorized access attempts, malware, and network attacks.
- **Incident Reporting and Response**: Any suspected security incidents (e.g., unauthorized access, data breaches, malware) must be reported immediately to the designated security team. A well-defined incident response plan will be followed to contain, mitigate, and investigate such incidents.
- **Post-Incident Review**: After any security breach or incident, a review will be conducted to determine the root cause, response effectiveness, and necessary corrective actions to strengthen security measures.

6. Network and Infrastructure Security

- **Firewall and Perimeter Security**: Firewalls and other perimeter security measures will be implemented to prevent unauthorized access to internal networks and resources.
- **Network Segmentation**: Sensitive data and systems will be isolated in secure network zones, limiting access to authorized personnel only.
- **Secure Communication**: All sensitive communication over the network will be encrypted using secure protocols such as HTTPS, TLS, and VPNs for remote access.

7. Software and System Security

- **Patch Management**: All software and systems will be kept up to date with the latest security patches. Updates will be tested and deployed in a timely manner to address known vulnerabilities.
- **Secure Development**: Secure coding practices will be enforced in the development of internal and external applications. Regular code reviews and security testing (e.g., penetration testing) will be conducted to identify and resolve security flaws.
- **Third-Party Services**: Before integrating third-party tools, services, or software, a security review will be conducted to ensure they meet **bvda.co.uk**'s security standards.

8. Employee Security Awareness

- **Training**: All employees will receive regular cybersecurity training, including awareness of phishing, social engineering attacks, password hygiene, and secure use of company devices and networks.
- **Policy Acknowledgment**: Employees will acknowledge their understanding of security policies and procedures, including acceptable use policies, and will be expected to comply at all times.

9. Physical Security

- **Data Center Security**: Data centers and other critical infrastructure will be secured with physical controls, including access restrictions, video surveillance, and monitoring systems.
- **Device Security**: All company devices (laptops, mobile devices, etc.) will be secured with encryption, strong passwords, and remote wipe capabilities in case of loss or theft.

10. Compliance and Legal Requirements

- **Regulatory Compliance**: **bvda.co.uk** will comply with applicable data protection and cybersecurity regulations, including GDPR (for EU and UK users), the Data Protection Act 2018, and other relevant industry standards such as ISO 27001, PCI-DSS (if applicable), and NIST.
- **Audits**: Regular internal and external security audits will be conducted to assess compliance and identify areas for improvement.
- **Third-Party Agreements**: Security standards will be defined and enforced in contracts with third-party vendors, especially those handling sensitive data.

11. Continuous Improvement

- **Ongoing Risk Assessment**: Regular risk assessments will be conducted to evaluate new and emerging threats, adjusting policies and controls as necessary.
- **Feedback and Improvements**: Feedback from employees, audits, and security incidents will be used to continuously improve security practices.

12. Review and Updates

This security policy will be reviewed and updated on an annual basis or sooner if there are significant changes in the business environment or security landscape.