Information Security Policy

1. INTRODUCTION

We are REVELTRY, an application provided and maintained by Wondr Technologies UK Limited (company number 16979480) ("we", "us" or"our") of C/O Gs Verde Accountants The Mezzanine, 1 The Square,Bristol, City Of Bristol, United Kingdom, BS1 6DG.

2. Scope

The scope of this Information Security Policy includes, but is not limited to:

1. All information processed by us in pursuit of our operational activities, regardless of whether it is processed electronically, or in paper form including but not limited to:
i. External customer information;
ii. Operational documents, plans and minutes;
iii. Financial, compliance, and other company records;
iv. Employee records.

2. All information processing facilities used in support of our operational activities to store, process, transmit or otherwise interact with information;

3. All external organizations that provide services to us in respect of information processing facilities. This Policy applies to all employees, consultants, contractors and third parties engaged by us (collectively referred to as “users”). All users shall read, understand, and comply with this Policy when storing, processing, communicating or otherwise interacting with information in the course of performing their duties.

All users shall comply with all controls, practises, protocols, and training to ensure such compliance. Any breach of this Policy may result in disciplinary or regulatory action.

3. Data Protection Accountability

Wondr Technologies UK Limited is the data controller responsible for ensuring that personal data is processed in compliance with applicable data protection laws, including the UK GDPR and the Data Protection Act 2018.Senior management retains overall accountability for information security and data protection compliance.

4. Definitions

Information security is aimed at protecting the following three attributes of our information:

i. Confidentiality- ensuring information assets are not accessible by or disclosed to unauthorized individuals, entities, or processes;
ii. Integrity- ensuring the accuracy and completeness of information assets;
iii. Availability- ensuring information assets are accessible and usable upon demand by an authorised entity.

Information asset – any information and information processing facility that has value to us.

Information owner – an individual accountable for the information asset.

Information processing facilities – any information processing system, service, or infrastructure, or the physical locations housing them.

5. Risks

A lack of information security can lead to incidents such as breaches of confidentiality,corruption of information and availability issues which could adversely affect our reputation and that of our customers along with our ability to meet contractual, legal, and regulatory obligations. Without defined and measurable objectives, it is not possible to determine whether our information security activities meet the intended outcomes.

6. Objectives

The objective of this Information Security Policy is to enable us to effectively manage any identified and relevant information security threats in order to meet our strategic business goals and to maintain its legal, regulatory, and contractual compliance obligations. The security controls are designed to mitigate all information security-related threats, whether external or internal, as well as deliberate or accidental.

Compliance with this Information Security Policy is necessary to ensure business continuity, and minimize business damage by preventing or reducing the likelihood of information security incidents occurring, and minimizing their impact should they occur.

In support of this Information Security Policy, our Senior Management Team (SMT) accepts its role in being fully accountable for information security and is committed to:

i. Managing and reducing information security risk in an informed manner;
ii. Minimizing the impact on us when information security incidents occur
iii. Ensuring that we have identified applicable, legal, regulatory, and contractual requirements and that they are complied with.

7. Responsibilities

Our management shall be accountable for ensuring that appropriate security and compliance controls are identified, implemented and maintained by information asset owners. It shall be supported in this task by the Information Security Forum (ISF).

Our ISMS manager shall be responsible for managing information security at an operational level and for providing advice and guidance on its implementation and is responsible for:

i. Ensuring that the Information Security Policy is reviewed at least every 12 months and in response to any significant changes. Where significant changes do occur, these shall be made known to all users;

ii. Establishing procedures to implement this and other policies within the company and for monitoring compliance;

iii. Ensuring appropriate training is provided to information asset owners, custodians and users, as well as network and system administrators.

Unless explicitly delegated to another position, the Director is the appointed decision maker for risk and vulnerability analysis as well as the management of information and incidents. For each of these specific areas, dedicated policies and procedures shall provide greater detail on role requirements. In the absence of the ISMS Manager, all of their responsibilities are transferred automatically to the Director, unless explicitly delegated to another role.

Information asset owners within our company shall be responsible for the identification,implementation and maintenance of controls that are commensurate with the value of the information assets they own and the risks to which they are exposed, and for periodical review identified based on the asset value.

It is the responsibility of all users to adhere to this Information Security Policy and to report information security incidents and events to their closest leader and the ISMS manager as soon as possible. Non-compliance with this Information Security Policy or other information security related policies by any user may result in disciplinary action being taken.

8. Policy

Under this Information Security Policy, we shall ensure that the following information security requirements are complied with:

• Information assets and information processing facilities are protected against unauthorized access;

• Information is protected from unauthorized disclosure;

• Confidentiality of information assets is maintained;

• Integrity of information assets is maintained;

• Our requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities are met;

• Statutory and expressed or implied legal obligations are met;

• Regulatory,contractual, and internal compliance obligations are met;

• Requirements for the continuity of information security are determined and maintained within our business continuity arrangements;

• Unauthorized use of information assets and information processing facilities is prohibited,and the use of obscene, racist, or otherwise offensive statements is dealt within accordance with other appropriate policies published by us;

• This Information Security Policy is communicated to all users, for whom information security training shall be provided where necessary;

• A systematic approach to information security risk management is followed and is a continual and dynamic process;

• Information security is managed through a formal information security management system(ISMS) that is defined within a documented framework;

• The performance of the ISMS and the effectiveness of information security controls is continuously improved;

• All breaches of information security, actual or suspected, are reported and investigated inline with our published policies and procedures;

• Controls are commensurate with the risks faced by us.

In support of this Information Security Policy, more detailed operational security policies and processes shall be developed for users, information assets and information processing facilities. These supporting policies shall be reviewed at planned intervals or if significant changes occur to ensure their continued suitability, adequacy, and effectiveness.

Any exceptions or deviations from the requirements of this Information Security Policy shall be authorised by the ISF. Any such deviations or exceptions shall be managed through our incident management or change management processes.

9. Compliance Monitoring

Information security objectives shall be agreed on an annual basis, supported by a set of key performance indicators (KPIs), with milestones and targets being set as appropriate. These measures shall be reported to the ISF for review.

10. Data Protection and UKGDPR Compliance

We processes personal data in accordance with the UK GDPR and the Data Protection Act 2018.Personal data shall be:

- Collected for specific and lawful purposes;
- Limited to what is necessary (data minimisation);
- Stored securely with appropriate safeguards; and
- Accessible only to authorised personnel on a need-to-know basis.

Personal data and system logs shall be retained only for as long as necessary for security, legal, and operational purposes, and in accordance with our Data Retention Policy.

11. Access Control and Authentication

Access to systems and data shall be restricted through:

- Role-Based Access Control (RBAC) and least-privilege principles;
- Multi-Factor Authentication (MFA) for privileged and administrative access; and
- Periodic access reviews and prompt revocation upon role change or termination.

12. Incident Response and Breach Notification

All security incidents must be reported promptly and managed in accordance with our incident response procedures.

We shall:

• Investigate,contain, and remediate incidents; and
• Assess and comply with UK GDPR breach notification obligations, including reporting to the ICO within 72 hours where required.

13. Third-Party Vendor

Security Third-party providers shall be subject to appropriate security due diligence and contractual data protection obligations.

Access to Company systems or data shall be limited, controlled, and periodically reviewed.

14. Secure Development and Application Security

We shall follow secure development practices, including:
• Code reviews and vulnerability testing;
• Monitoring of dependencies; and
• Timely remediation of identified vulnerabilities.

Controls shall be implemented to prevent misuse or exploitation of platform functionality.

15. Logging, Monitoring, and Fraud Detection.

We shall maintain logging and monitoring of key systems, including user activity, administrative actions, and transactions.

Monitoring controls shall support the detection of unauthorised access, suspicious activity, and potential fraud.

16. Backup, Disaster Recovery, and Business Continuity.

Critical systems and data shall be regularly backed up and protected.

Recovery procedures shall be maintained and tested periodically to ensure timely restoration and continuity of services.

17. Security Awareness and Training

Employees and relevant contractors shall receive periodic training on information security and data protection.

Training shall include awareness of phishing, social engineering, secure data handling, and incident reporting responsibilities.

18. Changes to this Policy

This Information Security Policy shall be reviewed on an annual basis by the ISF.

The Policy may also be updated periodically when necessary to ensure that it remains up to date, appropriate and consistent with our strategic business objectives.

Changes to this Policy shall be communicated to all users.