Data Security Policy

1 INTRODUCTION

1.1 This policy (the "**Policy**") sets out the approach of V.Group to data security.

1.2 This Policy:

(a) forms part of V.Group's Compliance & Ethics Policies which are available at https://vgrouplimited.com/legal/compliance/;

(b) applies to all Colleagues;

(c) has been approved by the Head of Information Systems of V.Group;

(d) should be read in conjunction with V.Group's Information Systems Policies & Procedures which can be accessed via VNet; and

(e) may be amended by V.Group at any time, consistent with the requirements of applicable laws and regulations. Any revisions will take effect from the date on which the amended Policy is published, as indicated by the version number.

1.3 Any breach of this Policy will be taken seriously and may result in disciplinary action.

1.4 Any questions or concerns about the operation of this Policy, including whether this Policy has been followed, should be referred to Group Legal by contacting legal@vgrouplimited.com

2 DEFINITIONS

2.1 "**Colleague**" means any employee of V.Group or any person engaged by V.Group;

"**Group IS**" means the information systems function of V.Group (which may be contacted via ohelp@vships.com); and

"**V.Group**" means Vouvray Acquisition Ltd and its subsidiaries and/or affiliates.

2.2 Words denoting the singular shall include the plural and vice versa.

3 WHAT IS DATA SECURITY?

3.1 Data security is ensuring the confidentiality, availability and integrity of data – this is vital to operations and reputations of V.Group and third parties it deals with.

3.2 Data security applies to:

(a) physical and electronic data; and

(b) both personal and other data (business data or otherwise).

NB: If data is **Personal Data**, please see the Data Protection Policy at https://vgrouplimited.com/data-protection-overview/ for guidance.

4 CONSEQUENCES OF BREACH

4.1 Any breach of data security can result in V.Group being unable to carry out its functions effectively, claims being made by third parties, and could cause significant and long-term harm to V.Group's operations and reputation

5 WHAT IS A DATA SECURITY BREACH?

5.1 A "**Data Security Breach**" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, data.

5.2 Examples of Data Security Breaches are:

(a) "Confidentiality breach" – an unauthorised or accidental disclosure of or access to data;

(b) "Availability breach" – an unauthorised or accidental loss of access to or destruction of data;

(c) "Integrity breach" – an unauthorised or accidental alteration of data.

6 PHYSICAL SECURITY AND ACCESS CONTROLS

6.1 Colleagues must take appropriate measures to prevent any Data Security Breaches which may affect the confidentiality, availability or integrity of data.

6.2 Physical security

(a) Colleagues must take appropriate physical security measures to protect data.

(b) Such measures include: building access controls, access to computers, laptops, mobile and other work devices, preventing inadvertent viewing or access to data whether onsite, offsite or travelling.

6.3 Access controls

(a) Group IS puts in place access controls to systems but Colleagues must also ensure that appropriate access controls are put in place, e.g. where new technologies are used.

(b) Such measures include: password-protection, not disclosing passwords to unauthorised persons, encrypting highly confidential data.

6.4 Colleagues must only use work devices (e.g. computers, laptops, mobiles) for work and handling work data – use of personal devices is prohibited.

7 DATA SECURITY BREACH AND DATA SECURITY INCIDENT

7.1 Paragraph 5.1 defines what a Data Security Breach is.

7.2 A "**Data Security Incident**" is a possible, potential or suspected Data Security Breach. It is essential that you understand the distinction between a Data Security Breach and a

Data Security Incident, i.e. a Data Security Incident is not necessarily a Data Security Breach.

7.3 If there has been a Data Security Incident, any Colleagues involved should refer to the Data Security Incident as an "incident" and should not refer to it as a "breach" (particularly when communicating in writing/by email).

7.4 It is for Group IS to determine whether a Data Security Incident constitutes a Data Security Breach.

8 NOTIFICATION OF A DATA SECURITY INCIDENT

8.1 Notify Group IS

(a) **You must report all Data Security Incidents (i.e. all *possible, potential or suspected* Personal Data Breaches) to Group IS immediately and in any event within 24 hours of becoming aware of the Data Security Incident**.

NB: If the incident is a **Personal Data** Incident, please see the Personal Data Incident Notification Policy at https://vgrouplimited.com/data-protection-overview/ for the correct process.

(b) If in doubt as to whether a Data Security Incident or Data Security Breach has occurred, you are required to err on the side of caution and report it.

(c) The Data Security Incident notification needs to be made via IT Connect.

8.2 Group IS will investigate and advise accordingly.

9 ACCEPTABLE USE POLICY

9.1 Colleagues, by accessing V.Group's systems, accept V.Group's Acceptable Use Policy contained in the Information Systems Policies & Procedures which can be accessed via VNet.

10 SYSTEM MONITORING

10.1 Unless otherwise stated, V.Group owns all rights in physical and electronic data, emails and other communications. By using such V.Group data, users do not, and are not intended to, acquire rights in that data.

10.2 To ensure compliance with this Policy, V.Group has systems in place allowing V.Group to monitor communications, the use of its systems and access to data. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

10.3 The Company reserves the right to retrieve the contents of messages or check searches which have been made on the internet for purposes including:

(a) to monitor whether the use of systems complies with this Policy;

(b) to find lost messages; and

(c) to assist in investigations or to comply with legal obligations.

11 RELEVANT POLICIES

11.1 V.Group has the following policies in place which help support the effectiveness of this Policy and should be referred to as appropriate:

(a) Data Protection Policy (https://vgrouplimited.com/data-protection-overview/); and

(b) Social Media Policy (https://vgrouplimited.com/legal/compliance/).

12 INTERNAL REPORTING

12.1 You must immediately contact Group IS if any of the following occur:

(a) as required under this Policy; or

(b) if there is any actual or suspected breach of this Policy.

13 DOCUMENT CONTROL

13.1 The Head of Information Systems of V.Group is the owner of this Policy and is responsible for ensuring that it is reviewed in line with the relevant review requirements.

13.2 A current version of this Policy is available at https://vgrouplimited.com/legal/compliance/

13.3 This Policy was approved as stated in this Paragraph and is issued on a version-controlled basis.

Version	Date of Issue	Approved by	Position
1	30.09.2019	Derek Rose	Head of Information Systems