# INFORMATION SECURITY POLICY

| DOCUMENT OWNER | APPROVED BY | DATE |
| --- | --- | --- |
| Chief Security Officer | Managing Director | 24/05/2024 |

# CONTENTS

# 1. PURPOSE

This policy outlines Vertex Professional Services (the “Company”) approach to information security management and provides the guiding principles and responsibilities to ensure our information security objectives are met. It applies to any person and/or organisation who in the official discharge of their duties requires access to the Company’s or our customers information.

# 2. INTRODUCTION

Failure to adequately secure our own or our customers information could result in significant liability for the Company leading to either financial, legal, and/or reputational damage. This Information Security Policy has been written to ensure that the confidentiality, integrity, and availability of the Company, and our customers information, is stored, processed, shared, and more generally managed appropriately.

# 3. OBJECTIVES

The objectives of this policy are to:

1. Ensure safeguards are in place to protect the Company and its customers information from both internal and external security threats that could negatively impact business operations, our financial position and reputation.
2. To ensure our business continuity and disaster recovery operations are adequate by deploying proportionate security tools to detect, respond and to recover from an incident.
3. Ensure compliance standards are met, maintained, and regularly reviewed with regard our legislative, regulatory, and/or contractual landscape for information security and data protection.
4. Ensure that the principles of Governance, Risk and Compliance (GRC) are effectively managed through a robust Security Risk Management (SRM) regime, which is fully endorsed by the Company’s Senior Leadership Team (SLT).
5. To foster and maintain a positive security culture for the Company through:
    - The provision of clearly defined information security roles and responsibilities.
    - That all users of our systems (the “User Community”) clearly understand their roles and responsibilities with regard information security.
    - That appropriate advice, guidance, and training is provided to the User Community to understand and raise awareness of security threats.
    - To ensure that any security violations are reported on in a timely manner, are dealt with promptly and to prevent a security incident from further escalation.

# 4. SCOPE

This policy is applicable to anyone and/or organisation who in the discharge of their official duties requires authorised access to the Company’s Information Communications Technology (ICT) and more generally any information bearing assets. This includes, but is not limited to:

1. All facilities, technologies and services that are used to process and or store the Company’s and/or our customers information.
2. All authorised information bearing assets or mobile devices connected to any of our networks and/or which contain Company and/or customer information.
3. All information processed, accessed, shared, manipulated, or stored (in any format) by the Company pursuant to its operational activities.
4. Data over which the Company is the Data Controller or Data Processor (wherever held).
5. All external parties that provide information processing services to the Company.

# 5. POLICY

All information being processed, be that digital and/or in hard copy, shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability and to ensure appropriate legal, regulatory, and contractual obligations are being met. The following principles provide the overarching governance for the security and management of information:

1. GRC activities are undertaken and are escalated, where applicable, to the SLT for further action – refer to document SRF 1.1 Security Charter.
2. Access to information shall be based on the notion of least privilege, additionally ensuring that the 'need to know' and 'need to share' principles are rigorously enforced, and that separation of duties are upheld – refer to documents SRF 1.2 Access Control Policy and SRF 1.3 Separation of Duties Policy.
3. Information security provision and the policies that guide it will be regularly reviewed, supported by a minimum annual external audit and penetration testing as specified by the Security Steering Committee (SSC) – refer to document Information Governance (IG) IG 16 ToR SSC.
4. Ensure that the User Community attend the appropriate information security, insider threat and data protection training on induction to the Company and annually thereafter (this also includes bespoke security training for employees with specific security and/or data protection responsibilities) through a security programme of activities – refer to document – SRF 1.4 Security Education Training Awareness Policy
5. Any type of security incident is reported to the Security Operating Authority (SOA). in a timely manner - refer to SRF 1.5 Security Incident Reporting Policy.
6. All information (data) shall be managed in accordance with the Company's Information Governance (IG) Framework. The IG requirements are contained within IG 1.0 Information Governance Policy and associated sub- policies. All employees must familiarise themselves with the IG Framework.

The User Community shall ensure that this Information Security Policy, and the Company's Acceptable Use Policy is understood, acknowledged, and adhered to – refer to document SRF 1.6 Acceptable Use Policy.

# 6. LEGAL AND REGULATORY OBLIGATIONS

The Company has a responsibility to abide by and adhere to all current UK and EU legislation as well as regulatory and contractual requirements. A non-exhaustive summary of legislation that contributes to the form and content of this policy is provided in Appendix A.

## 6.1 COMPLIANCE

The Company will conduct information security compliance and assurance activities, facilitated by the Company's SOA. This will ensure that:

1. Information security objectives are being monitored and met.
2. Continuous measurement and improvements are made with regard the information security programme.

Compliance with this policy is mandatory. Any violation of this Information Security Policy shall be investigated and treated extremely seriously by the Company, which in severe cases could lead to termination of employment. Any security breach will be managed in accordance with all relevant Company policies, including the appropriate disciplinary policy, which is aligned with the Security Breach Management process – refer to document SRF 1.7 Statement of Intent.

## 6.2 INFORMATION CLASSIFICATION

The following table provides a summary of the information classification levels that the Company have adopted, and which underpin our information security principles. These classification levels explicitly incorporate the UK/ EU General Data Protection Regulation definitions of 'Personal Data' and 'Special

Categories' of Personal Data, as laid out in the Company's IG 2.0 Data Protection Policy. These principles also account for the security controls applicable to other classifications of information the Company manage. The document Information Governance (IG) 10 Data Classification Standard provides a more detailed description on our security classification levels and the requisite handling instructions the User Community shall follow.

| Security Level | Definition | Examples | FOIA2000 status |
|---|---|---|---|
| Strictly Private | Accessible only to specified staff members, this data is defined by the 'Need to Know' & "Need to Share" (NTK) principle. This level of data must be controlled through appropriate technical and organisational measures, which includes encryption at rest, during transit and other technical and non-technical security controls. | 1. GDPR-defined Special Categories of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record) including as used as part of primary or secondary research.<br>2. UK Government/ NATO and/ or other governmental related data.<br>3. Password and account information.<br>4. Sensitive HR data.<br>5. Financial data related to the Payment Card Industry Data Security Standard. | Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations. |
| Private | Normally accessible to specified staff members only, this data is defined by the 'Need to Know' & "Need to Share" (NTK) principle. This level of data should be controlled through appropriate technical and organisational measures, which includes encryption at rest and during transit. | 1. Personal data.<br>2. Propriety information<br>3. Copyright<br>4. Intellectual property<br>5. Sensitive financial reports<br>6. Business mergers<br>7. Business strategy, reports, contracts, and proposals<br>8. Competitor and customer<br>9. HR & Apprentice data. | Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations. |
| Public | Accessible to all members of the public. | Any information that is available through Open Source. Always ask if you are unsure. | Freely available on the website and other open sources. |

## 6.3 SUPPLIERS

All suppliers of services, including any Cloud services, must abide by the Company's Information Security Policy, or otherwise be able to demonstrate corporate security policies and / or appropriate information security certifications (e.g. ISO27001, Cyber Essentials Plus) providing equivalent levels of assurances. This includes:

- All instances when accessing or processing VPS and/or our customer's information, whether on site or remotely.
- When subcontracting to other suppliers for Private and Strictly Private information.

Refer to document SRF 1.8 Supply Chain Security Policy.

### 6.4 INCIDENT HANDLING

Information must be managed appropriately across the Company by the relevant stakeholder (s). The Company is under a legal obligation to report certain information and/or data breaches within specific timelines. This requires all our employees to remain vigilant and always report any information security incident to the SOA in a timely manner and as soon as it is safe to do so. There are several ways to report a security incident which include:

By creating a ticket using your Company device - EMEA IT Helpdesk , choosing ticket type "Information Security" (for further information please see Reporting Information Security Incidents).

By sending an e- mail to VPSsecurity@gov2x.eu.

If the situation is urgent and cannot wait by telephone - +44 (0) 7731987312.

Breaches of personal data will be reported to the Information Commissioner's Office, or other appropriate supervisory authority by the Company's Data Protection Officer (DPO). The DPO can be contacted at privacy.EMEA@gov2x.eu (shared mailbox), or if confidential in nature directly to the DOP: kharkett@gov2x.eu

All employees must report instances of actual or suspected phishing to VPSITsecurity@gov2x.eu.

## 7. RESPONSIBILITIES

The information below defines the User Community responsibility, which is supplemented further by table 1 and defines the roles and responsibilities for information security.

### 7.1 GENERAL USERS WITH RESPONSIBILITIES FOR INFORMATION MUST:

1. Handle that information in accordance with its classification level - refer to document IG 10 Data Classification Standard.
2. Abide by the Company security policies, procedures, and any contractual security and data protection requirements as stipulated through contracts.
3. Ensure that all breaches of security, including any Personal Data breaches, are reported in a timely manner to the appropriate stakeholder – refer to SRF 1.5 Security Incident Reporting Policy.
4. Ensure that information security is an integral part of our own and our supply chain procurement lifecycle (from concept to disposal/termination) - refer to document SRF 1.8 Supply Chain Security Policy.
5. Ensure that their authentication information (e.g. passwords) are adequately protected and that access to any ICT is in accordance with the Company's SRF 1.9 Password Policy and SRF 1.2 Access Control Policy, respectively.
6. Ensure proper and effective use of cryptography to protect confidentiality, authenticity, and/or integrity of information and to ensure that secure file transfer and/or encryption is deployed to maintain the security of information transferred internally and externally. – refer to SRF 1.10 Encryption Standard.
7. Prevent unauthorised physical access, damage and interference to the Company's information and information processing facilities – refer to SRF 1.11 Mobile Working Device Policy.

### 7.2 IT STAFF WITH RESPONSIBILITIES FOR INFORMATION SECURITY MUST IN ADDITION TO 7.1:

1. Ensure backup information to protect against the loss of data, and additionally store the backup in separate locations to the information systems.
2. Conduct logging and monitoring activities to detect anomalies, report and generate evidence and to conduct security investigations, where authorised, with regard any identified policy violations.
3. Control operational software and applications to ensure the integrity of operational systems.

4. Conduct technical vulnerability assessments in line with external driver requirements.
5. Ensure that information security is an integral part of information systems throughout their lifecycle (from concept to disposal/termination).

## 7.3 PROCUREMENT TEAM MUST IN ADDITION TO 7.1:

Ensure any requests for purchase of IT services, software, hardware, and cloud contracts have been authorised by security and IT.

## 7.4 INFORMATION ASSET OWNERS/ MANAGERS MUST IN ADDITION TO 7.1:

Responsible for their specific area of responsibility, including all the supporting information and documentation that may include working documents/ contracts/ customer/ employee or apprentice information.

Refer to documents:

6. Information Governance (IG) 1.0 IG Policy.
7. IG 18 ToR IAO.
8. IG 19 ToR IAM.

## 7.5 DATA PROTECTION OFFICER (DPO) MUST IN ADDITION TO 7.1:

1. Responsible for data protection and records retention issues.
2. Breach reporting to the supervisory authority.

Refer to document IG 1.22 ToR DPO.

## 7.6 TECHNOLOGY TEAMS MUST IN ADDITION TO 7.1:

Responsible for the information systems (e.g. HR/ / Finance/ Cornerstone etc.) that support Company work. This includes:

1. Ensure that data is appropriately stored and protected.
2. That the risks to data are appropriately understood and mitigated through escalation process to security.
3. That the identity access management activities are implemented, are appropriate, that separation of duties is enforced meaning that data is only accessible to the right people (need to know), shared with only those that need to know (need to share) and ensuring, in conjunction with IT, there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

***Table 1: RACI Chart: Responsible, Accountable, Consulted & Informed***

| Requirement | R | A | C | I |
|---|---|---|---|---|
| Operational authority for information security, including the development, review and continuous improvement of the information security plan and security management directives that underpin the necessary controls. | Chief Security Officer (CSO) | Managing Director (MD) | Senior Leadership Team (SLT) | IT Department |
| Security Risk Management. | CSO | MD | SLT | Contracting Authority (CA) |
| Implementation of Cyber security risk profile and recommended activities to mitigate risks. | Information Asset Manager (IAM) | Information Asset Owner (IAO) | CSO | SLT |

| | | | | |
|---|---|---|---|---|
| Implementation of technical controls. | IT Manager | Head of Learning Solutions | CSO | SLT |
| Understanding what information is being processed, where it is and who has access. | IAM | IAO | CSO | SLT |
| Security Breach Management & Investigation. | CSO | CSO | Head of HR | SLT |

### 7.7 SUPPORTING POLICIES, PROCEDURES, CODE OF CONDUCT, STANDARDS AND PRACTICES

Supporting policies have been developed to strengthen and reinforce this policy statement. These security management directives form part of the Company's Security Reliability Framework (SRF) and is applicable to anyone and/or organisation. The SRF documents, along with associated codes of practice, procedures and guidelines are published on the Company's Policies and Procedures website, along with the Company's Information Governance Framework.

All employees, consultants, contractors and any third parties authorised to access the Company's network or computing facilities are required to familiarise themselves with these sub-policies and procedures and to adhere to them in the working environment.

Where a person does not understand, or disagrees with a particular policy, for example, it is unworkable for them and as a result negatively impacts on the operational effectiveness of the work, they are actively encouraged to speak with the SOA.

## 8. REVIEW AND DEVELOPMENT

This policy will be reviewed minimum annually by the Company's Security Steering Committee and updated regularly to ensure it remains appropriate in the light of any relevant changes to the law, organisational policies, or contractual obligations.

## APPENDIX A: SUMMARY OF RELEVANT LEGISLATION

### OFFICIAL Secret Act 1989

The Official Secrets Acts 1911-1989 provide the main legal protection in the UK against espionage and the unauthorised disclosure of information.

### The Computer Misuse Act 1990

Defines offences in relation to the misuse of computers as:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

### The Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA2000) is a general right of public access to all types of recorded information held by public authorities to promote a culture of openness and accountability.

### Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

### Defamation Act 1996

“Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm.1

### Obscene Publications Act 1959 and 1964

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape, or torture.2

### Protection of Children Act 1978, Criminal Justice Act 1988, Criminal Justice, and Immigration Act 2008

The Protection of Children Act 1978 prevents the exploitation of children by making indecent photographs of them and penalises the distribution and showing of such indecent photographs. Organisations must take appropriate steps to prevent such illegal activities by their workers using their digital systems and networks.

The definition of ‘photographs’ include data stored on a computer disc or by other electronic means which is capable of conversion into an image. It is an offence for a person to […] distribute or show such indecent photographs; or to possess such indecent photographs, with a view to their being distributed or shown by himself or others.

### Terrorism Act 2006

The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation, or instigation of acts of terrorism. It also prohibits the writing, publication or circulation of information which is likely to be useful to any one or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful. In addition, it prohibits the glorification of the commission or preparation

(whether in the past, in the future or generally) of terrorist acts or such offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.

### Counter-Terrorism and Security Act 2015 – Statutory Guidance

The statutory guidance accompanying the Counterterrorism and Security Act 2015 (Prevent duty guidance for higher education institutions in England and Wales Prevent duty guidance: England and Wales (2023) - GOV.UK (www.gov.uk) requires VPS, trading under Vertex Company UK 1 Limited to have "due regard to the need to prevent people from being drawn into terrorism." The Act imposes certain duties under the Prevent programme, which is aimed at responding to "the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views." The Prevent programme also aims to provide "practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support." The Company must balance its existing legal commitments to uphold academic freedom and (under the Education (No. 2) Act 1986) freedom of speech within the law against the new Prevent duty and seek to ensure that its IT facilities are not used to draw people into terrorism.

### General Data Protection Regulation and DPA 2018

The GDPR has applied to the UK from 25 May 2018, and has been passed explicitly into UK law. The UK GDPR reinforces and extends data subjects' rights as laid out in the Data Protection Act (1998), and provides additional stipulations around accountability and governance, breach notification and transfer of data. The UK/ EU GDPR requires VPS to maintain its Records of Processing Activities (ROPA) to ensure where personal data is voluntarily gathered people are required to explicitly opt in and can also easily opt out. It requires data breaches to be reported to the Information Commissioner's Office and/or respective supervisory authority within the European Economic Area within 72hrs of the Company becoming aware of their existence. Further information is contained within the Company's Privacy Framework.

## VERSION CONTROL

| Version No | Date | Classification | Owner | Approver |
|---|---|---|---|---|
| Ver 1.3 | 03/06/2024 | Private | CSO | MD |