Information Security and Privacy Policy
Reviewed on 24 May 2022

As a leading Channel-first cloud service provider, virtualDCS has contracts with organisations across Europe. These customers expect that we demonstrate the upmost professionalism in the security and privacy of our processes, and systems.

Specific, subsidiary Standard Operating Procedures are considered part of this information security policy and have equal standing.

This policy is authorised by the Board, and it is reviewed and updated when necessary.

In this document VirtualDCS may be referred to as “we”, “us”, or “our”.

1. Introduction

virtualDCS is a provider of Channel-first cloud computing services, specifically VMware-based products. We have designed, built, and maintained a ‘Virtual Platform’ that supports business computing in the UK and Europe. Our clients range from international retail chains, through to local micro businesses.

To provide our services, we must collect, and process data. To protect this data, we have implemented an Information Security Management System, that has been certified to ISO 27001:2013, by BSI. Our management system is mature, and has been certified since 2015.

This policy describes our approach to information security and privacy, and acts as a reference document for our staff, customers, and the public.

2. Our Stakeholders

Our staff, customers, and the public expect the very best from our company on technological and procedural matters. They trust us to protect the confidentiality, integrity, and availability of their data and their virtual machines.

We have entered into multiple contractual agreements with customers, which specifically require us to maintain strict physical and information security. We also have legislative requirements under UK law.

Our stakeholders include: our staff; contractors; customers (including their customers and staff); our suppliers; our regulatory bodies (including UK and EU law enforcement, and UK administrative bodies); and our appointed auditors.

In addition to our contractual requirements, virtualDCS has a number of legal requirements placed upon it. These include (but are certainly not limited to): Data Protection Act 2018

(including the General Data Protection Regulations(GDPR); Computer Misuse Act 1990; Anti-Bribery Act 2010, 2021 Whistleblowing Policy. The Operations Director will keep abreast of these regulations and provide updates accordingly.

3. Our Information Security Management System

We have created an Information Security Management System, to structure our approach to security and governance. The scope of our ISMS, which has been certified to ISO 27001:2017, is:

The provision of safe and secure virtual server hosting services.

Our ISMS aims to provide a safe and secure environment for customers to host their virtual servers. Included in our scope are: the Virtual Platform Domain (VP); the physical servers it is operating from; both virtualDCS data centre locations (Derby, Leeds); and the back-office technical and administrative functions necessary for the operation of our services.

All virtualDCS staff, contractors and 3rd parties are in scope of the ISMS and receive training appropriate to their role.

Out of the scope of our ISMS are any assets used solely by customers and 3rd parties, such as a customer's virtual machine.

Where high levels of risk are identified, risk reduction or mitigation actions are documented and employed.

4. Proactive Security, and Commitment to Improvement

virtualDCS operates a 'proactive' security defence model. We have committed to continually improving the security and reliability of our platform: we own, control and when necessary, custom-build systems. We operate multi-zone environments to maximise uptime, redundancy, and to provide the fastest response time to customers. Our network architecture is designed to reduce single points of failure, and is constantly reviewed for best practice and compliance.

By approaching our platform architecture in this way, we can provide customers with the fastest and safest cloud environment.

Our platform is monitored 24x7x365 from our system centre, and by Pingdom. We monitor it for availability, reliability, and speed. A comprehensive external security testing programme is run every month to ensure that our service is secure from known exploits, new vulnerabilities, and targeted attacks.

5. Structured Approach to Managing Security

To ensure that we have a consistent approach to security and privacy for our stakeholders, we have created a number of Standard Operating Procedures that provide a formal process for our common tasks. These SOPs cover everything from User Passwords and Staff Vetting, through to Incident Response and Change Management.

Our SOPs are reviewed at least annually, and are updated in line with industry standards.

6. Privacy

VirtuaDCS takes its responsibility for protecting your data very seriously and we do advise you get to know our practices. If there's anything here you don't understand, or if you want to ask any questions, please feel free to contact us.

Who is the Data Controller?

We are Virtual Data Centre Services Ltd (virtualDCS).

Registered address: The Waterscape, 42 Leeds & Bradford Road, Leeds, West Yorkshire. LS5 3EG

Registration number: 10501907

What kinds of Personal Data does VirtualDCS Process?

VirtualDCS collects personal data for various purposes; with that in mind we have created a list of the types of personal data that we may collect, either directly from yourself or from other sources, in order to achieve those purposes.
The kinds of personal data we may collect include:

Customer / Client	Contact details,
Applicant / Temp / Volunteer / Intern	Contact details , CV
Partner / Member	Contact details
Supplier / Trader	Contact details, Bank details.

What are the reasons VirtualDCS collects Personal Data?

Legal Obligations

VirtualDCS uses personal data firstly to fulfil any contractual obligations that exist between us and yourself. Where we request personal data be provided to enter into, or meet the terms of any such contract, you will be required to provide the relevant personal data or we

will not be able to deliver the goods or services you want. In such cases the lawful basis of us processing the personal data is that it is necessary for the performance of a contract. We are required by law to process personal data for purposes relating to our legal obligations, these include:

- To provide for our financial commitments, or to relevant financial authorities.
- To comply with regulatory requirements and any self-regulatory schemes.
- To carry out required business operations and due diligence.
- To cooperate with relevant authorities for reporting criminal activity, or to detect and prevent fraud.
- To investigate any insurance claims, claims of unfair dismissal, claims of any kind of harassment or of discrimination, or any other claim whereby the organisation may have to defend itself.

Legitimate Interests

VirtualDCS may process Personal Data for any of the following purposes, which are considered to be within our legitimate business interests:

- To provide goods and services where it has been requested

Where does VirtualDCS obtain Personal Data from?

We will collect personal data directly from you in various ways. This could include:

- When you complete an online form, or if you provide the data directly to a representative of VirtualDCS.
- We collect some personal data from publicly accessible sources such as:
- LinkedIn for recruitment and sales.
- We may also gather personal data by any of the following methods:
- From technical functionality that gathers data automatically from computer equipment when people visit our online platforms.

Who will VirtualDCS share your Personal Data with?

To achieve the above stated purposes for which we process your personal data, we may have to share your personal data with certain third parties.

We shall make all reasonable efforts to ensure that any third-party we share your personal data with is also compliant with data protection law.

The kinds of third parties we may share your personal data with include:

- Organisation where it is necessary to provide goods or services.
- Organisations where it is necessary to setup various resources.

Where will VirtualDCS store your Personal Data?

VirtualDCS will not transfer your personal data to any country other than those that have been granted an adequacy decision under the General Data Protection Regulation.

We may however share your personal data with third-party organisations who then transfer the data. We shall take all reasonable measures to ensure those third parties are also compliant with data protection law.

How long will VirtualDCS keep your Personal Data?

We will keep your personal data only for as long as required to achieve the purposes for which it was collected, in line with this privacy notice.

The following criteria are what determine the period for which we will keep your personal data:

- Until we are no longer required to do so to comply with regulatory requirements or financial obligations.
- Until we are no longer required to do so by any law we are subject to.
- Until all purposes for which the data was originally gathered have become irrelevant or obsolete.

Your Rights, Our Responsibility

There are several rights granted to you immediately upon providing us with your personal information; some of these are mentioned above. We'd like you to know that at VirtualDCS we take your rights seriously and will always conduct ourselves in a way that is considerate of our responsibility to serve your legal rights.

The Right of Access

This grants you the right to confirm whether or not your personal data is being processed, and to be provided with relevant details of what those processing operations are and what personal data of yours is being processed.

If you would like access to the personal data we have about you, we ask that you contact us using the details below.

The Right to Rectification

This one is fairly straightforward; if you notice that the data we have about you is inaccurate or incomplete, you may request we rectify the mistake. We will make every effort to respond to requests of this type immediately.

The Right to Erasure

Otherwise known as the 'right to be forgotten', this given you the right to request your personal data be deleted.

This is not an absolute right; if you were to request that we erase your personal data, we would erase as much of that data as we could but may have to retain some information if it is necessary.

Were we have received a request for personal data to be erased, if it is necessary for us to retain some of that information we shall ensure that the remaining data is used only when and where it is absolutely necessary.

The Right to Objection

The right to object is a basic freedom all democracies enjoy. If you wish to object to the way we use, or have used, your personal data you may do so freely.

The Right to Portability

This is a legal right afforded to you that states we must pass on all of the details you have provided to us in a machine-readable format, either to your or to another provider of your choosing.

The Right to Complain

We will always try to maintain the highest standards and encourage the confidence our customers have in us as an organisation. To achieve this, we request that any complaints be first brought to our attention so we can properly investigate matters. If you would like to complain about VirtualDCS to a regulatory body, you may do so by contacting your local data protection supervisory authority.

Who is the VirtualDCS EU Representative?

Ametros Ltd
Lakeside Offices, Thorn Business Park, Hereford, England, HR2 6JT
0330 223 2246
Gdpr@ametrosgroup.com

7. Access Requests and Security Reports

Individuals in the European Union have the right to request access to, correction of, and in limited cases deletion of, their personal information.

If an individual wishes to submit a subject access request, they must email privacy@virtualdcs.co.uk, with specific details of the data they wish to review, and changes that need to be made.

virtualDCS will respond to subject access requests within 5 working days.

8. Supplier and Third-Party Applicability

virtualDCS requires its suppliers and associated third-parties to comply with this Policy. They must use appropriate policy and technical controls when accessing, transmitting, or storing our information assets. virtualDCS will audit supplier and third-party adherence to this policy from time to time.

9. Responsibility and Accountability

Overall accountability for information security and privacy rests with Richard May, on behalf of the company's Board.

Responsibility for many functions relating to security and privacy has been assigned to operational teams, including:

- **System security**
  The technical team, led by our Operations Director, John Murray, is responsible for ensuring that our systems are secure, and that they are designed and maintained according to our SOPs, and industry best practice.
- **Information governance, compliance, and standards**
  The virtualDCS information security management team is responsible governance, standards, and compliance issue. Further to this, we have trained an internal auditor to assist in the monitoring of these areas.
- **Information and document management**
  The administration team is responsible for managing the company's documentation library, across its computing and physical estate.

All virtualDCS staff are assigned some responsibility for information security and privacy, according to our Standard Operating Procedures. Each member of our team must ensure they are familiar with their responsibilities, and act accordingly.

10. Independent Audit

To ensure that we're meeting our obligations, and to provide our stakeholders with independent assurance of our performance, BSI performs regular audits on our Information Security Management System. These audits provide us with actionable feedback on our system, and enable us to continually improve our security and privacy.

Signed,

Richard May, Managing Director