



VIRTUS COMPLIANCE POLICY

Version 6.1

Document Control

Document Owner:	Kyle Morrison		
Author	Last Review Date	Next Review Date	Issue
Lenka Isajevova	23/06/2026	22/06/2027	6

Revision History

Change Date	Issue	Note
10/01/2023	1	First draft
19/12/2024	2	Document formatting update
02/02/2025	3	PCI DSS v4.0 scope inclusion
23/02/2025	4	ISO27001:2022 controls Migration
18/12/2025	5	Extension to scope
24/06/2026	6	NetZero commitment, Climate risk management, GHG emissions and environmental controls

VIRTUS Data Centres challenges the traditional data centre landscape in London with some fresh thinking. We go beyond traditional boundaries of data centre services. With every client we aim to become a valued, trusted and flexible partner in delivering their IT strategy.

We offer solutions for Enterprise IT as well as IT Services Providers, MSPs or Cloud providers. Every component is flexible, from the energy metering to dedicated or shared hall and plant, to self-service portal-based monitoring or fully managed services. Contracts can range from a day to a decade, and we offer the first Colocation-on-Demand and Connectivity-on-Demand services to the London market.

Above all, the breadth, depth, quality, flexibility and customer service of VIRTUS solutions delivers reduced Total Cost of Ownership of data centre and connectivity services when compared to alternatives. When combined with the convenience of our London locations – this is why VIRTUS data centres are becoming the preferred locations of growing business communities in London for IT, Cloud and Managed Services Providers, and Enterprise IT users in Finance, Media and Education.

VIRTUS' values underpin:

- Delivery of high-quality services designed to meet or exceed our customer's expectations;
- Our position as a leader at the forefront of the data centre industry, understanding the markets in which we operate, our future requirements and our customer's current and future requirements
- The on-going development of our people to enable delivery of high-quality outcomes
- Continual measurement, review and improvement of our policies, processes and service levels
- Protection of services and to the confidentiality, integrity and availability of the information we are supplied

VIRTUS is committed to operating in adherence to all applicable regulatory requirements, to meet or exceed customer requirements and continually improve the effectiveness of our management systems in line with the conditions of BS EN ISO9001:2015, BS EN ISO14001:2015, BS ISO45001:2018, BS EN ISO50001:2018, ISO/IEC 27001:2022, ISAE3000 Service Organisation Controls (SOC 2) Reporting, Information Technology Infrastructure Library (ITIL) Guidelines, BS ISO/IEC20000-1:2018 and BS EN ISO 22301:2019, and the Payment Card Industry Security Standard (PCI DSS) 4.0- Physical Security.



Senior Management Commitment:

Commitment to the delivery of quality, continual services, energy & environmental performance, health and safety and information security principles extends to senior levels of VIRTUS and will be demonstrated through this Compliance Policy. Senior Management shall guarantee the following:

1. The provision of appropriate resources to provide and develop/improve services, whether that is commercial, personnel, time or leadership resources
2. To ensure a systematic review of performance is conducted on a regular basis to ensure that service delivery, business continuity plans, energy & environmental and information security objectives are being met
3. To ensure that this policy and all contiguous controls are compatible with the strategic direction of the business and are integrated into the business processes.
4. Maintain a health and safety management system relevant to activities and processes covering all sites that:
 - a. Protects workers from reprisals when reporting hazards, risks and opportunities
 - b. Includes processes for consultation and participation of workers
 - c. Supports the functioning of health & safety committees.
5. To ensure that service delivery, energy & environmental and information security issues are identified, registered and treated as appropriate in a documented process
6. That a management review is conducted at least once annually and that business decisions are decided upon verifiable evidence
7. Utilise a risk-based approach for business decisions and determining operational controls
8. The appointment of competent and qualified responsibilities to manage processes & systems and to provide direction & support to persons (including managerial roles) contributing to the effectiveness of this policy and all contiguous controls in order to demonstrate leadership and commitment
9. To communicate the importance of effective policy & controls to preserve a culture of focussed improvement



With regards to providing quality, continual service, VIRTUS aims to:

- Achieve 100% compliance with customer service agreements
- All operational data centre space is appropriately and effectively managed
- Certify best practice security standards (physical, logical and personnel) are met by working closely with customers, key partners and suppliers and seeks ways in which we can continually improve our security to mitigate new vulnerabilities
- Ensure customers have confidence in our information security, and are safe in the knowledge that we are responsive to their security concerns
- Ensure customers have confidence in our business continuity arrangements to provide 99.9998% uptime of agreed service
- Meet or exceed every customer's requirements
- Gain and, where possible, act on feedback from our customers to enhance customer satisfaction
- Maintain and periodically test the suitability of emergency procedures and business continuity plans with a view to successfully dealing with service impacting incidences
- Ensure that processes and management systems are determined, documented and maintained to reflect our activities, compliance to applicable regulation and customer requirements, including the reporting of performance to senior management
- Establish and sustain high quality service reporting and notifications that is accurate
- Ensure service requests are handled competently and in a timely manner
- Strictly control the design, application and communication of changes within the data centre facilities
- Acknowledge, act on, resolve and communicate incidents in the most effective and practicable manner including the use of problem management for permanent close out and trending
- Ensure new data centres are indeed ready for service by undertaking controlled testing and commissioning and accurate handover to the Operations Department
- Ensure customer handovers are fulfilled and deemed effective within the specified time periods
- Provide an industry leading customer experience from pre-sales through to continuing service
- Understand and plan for the future needs of our customers
- Where possible, involve the latest, proven, best available technologies and techniques

With regards to relationships and partnerships, VIRTUS aims to:

- Build mutually beneficial relationships with our key partners to ensure that all outsourced activities within the company are effectively managed
- Where necessary, work with our key partners to improve services

- Ensure exceptional personnel competencies and personnel screening is achieved
- Request the use of mutually beneficial systems to promote collaborative working
- Regularly evaluate and monitor key partners using key performance indicators
- Communicate all necessary VIRTUS policies, processes and controls to key partners with receipt of understanding

With regards to business as usual, VIRTUS aims to:

- Utilise a risk-based approach to identify shortfalls or opportunities to further drive improvements within the company
- Determine requirements for monitoring and measuring performances, in order to make decisions based on facts and data
- Implement and maintain precise monitoring systems including (but not limited to) Building Management Systems, Power Management Systems and Information Management Systems
- Ensure relevant monitoring equipment is calibrated guaranteeing precise information
- Minimise (and prevent where possible) pollution arising from our activities & services and the activities of key partners through:
 - Improving environmental & energy performance by installing/implementing and maintaining efficient & effective infrastructure, policies, procedures and controls
 - Procuring 100% renewable energy sourced from sustainable grid power year on year for use within our data centres
 - Managing the storage of hazardous substances at our data centres, in particular diesel storage
 - Managing the safe collection of hazardous wastes from our data centres in accordance with waste hierarchies and compliant record management
 - Reducing the environmental impact of our office-based activities
 - Promote minimisation, reuse and recycling of wastes and to ensure diligent duty of care
 - Efficiently and accurately monitor and record diesel consumption for statutory reporting as to utilise FAME-free diesel wherever possible
- Compliant communication to government and industry bodies relating to permit, licences and company reporting requirements
- Operate efficient, safe and well-maintained data centres by:
 - Considering and addressing the environmental impacts of our activities and the activities of our key partners when planning and building new facilities and data centres in line with business requirements
 - Purchasing efficient products and services, and design for energy performance improvements



- Ensuring robust maintenance regimes are in place for maintaining suitable equipment and infrastructure to like-new conditions
- Using the best possible subcontractors (preferably manufacturers) to maintain equipment and infrastructure
- Diligently and, in a timely manner, act on statutory inspections report findings
- Audit and evaluate operational policies, processes, staff and controls through an audit schedule and communicating findings to senior management.

With regards to the people we influence, VIRTUS aims to:

- Identify competency requirements for our staff and provide adequate training, instruction, information and supervision to staff and others affected by our activities
- Provide internal, serviced communications systems that are appropriate for ongoing operations
- Adequately communicate and promote our Policies, processes and controls to all relevant parties
- Provide a suitable mechanism for feedback enabling staff to express shortcomings, opportunities to improve, non-conformances and additional controls.

Through the above aims, VIRTUS will determine and achieve business-driven objectives and continually improve our Service Delivery, Quality, Energy & Environmental, Health & Safety and Information Security performance.

Environmental, Sustainability and Climate Risk Management, VIRTUS aims to:

This section establishes the organisation's requirements for managing water usage (including closed loop and adiabatic systems), greenhouse gas (GHG) emissions, net zero commitments, and physical climate risks across all VIRTUS data centre . This will apply to all owned and operated data centres, critical infrastructure (cooling, power, water systems) third-party colocation and critical suppliers, only where applicable.



Greenhouse Gas Emissions Management

GHG Accounting (GHG protocol)

- Emissions shall be calculated and reported in accordance with the **GHG Protocol**, including:
 - **Scope 1:** On-site fuel combustion (e.g. standby generation) refrigerants and natural gas
 - **Scope 2:** Purchased electricity from Hydro, solar and wind sources
 - **Scope 3:** Supply chain, embodied carbon, and downstream impacts (where applicable)

Reduction Measures

- Renewable electricity procurement (REC's, PPAs)
- Continuous Energy efficiency improvements and investments (aligned to ISO 50001)
- Low-carbon fuels (HVO as transitional fuel, and white flame free Derv)
- Reduction of testing for backup generators and planning
- Selective Catalytic NOx reduction plant
- Low load strategy for cooling systems

Performance Targets

- Annual GHG reduction targets shall be defined and approved by ELT
- Carbon intensity metrics (e.g., tCO₂e per kWh) tracking and reporting
- Annual surveys conducted against ESOS and implementation and investment

Emissions data shall be subject to internal audit and, where required, **external assurance** for full verification and reporting requirements.

Net Zero Commitment

VIRTUS is committed to achieving net zero GHG emissions across its operations within a defined timeframe aligned with the board approved and reviewed NetZero roadmap

- **Net Zero Strategy**
 - A formal Net Zero roadmap shall be maintained and reviewed, including:
 - Interim reduction milestones (2030)
 - Final target date (2050)
 - The roadmap shall prioritise **absolute emissions reductions**, offsetting will be utilized where reduction is not applicable
- **Decarbonisation Hierarchy**
 1. Reduce energy consumption during growth and utilisation
 2. Improve efficiency (PUE optimisation) through monitoring and investment(LCA)
 3. 100% procurement of renewable energy
 4. Implement reduction into design near to zero as possible
 5. Use offsets only for residual emissions

- **Offsets and Residual Emissions**
 - Carbon offsets shall:
 - Be certified, regulated and verified
 - Only be used for residual, hard-to-abate emissions
 - Offsetting strategy must be transparent and documented.
- **Governance**
 - Net Zero progress shall be reviewed annually by ELT
 - Alignment with **CSRD, TCFD, and ESOS** is required where applicable.
- **Physical Climate Risk Management**
- **Policy Statement**

Physical Climate Risk Management

VIRTUS shall identify, assess, and mitigate **physical risks associated with climate change** to ensure resilience and impact of data centre operations.

Key Risks Considered

- Flooding (surface water)
- Extreme heat and seasonal effects impacting cooling capacity performance
- Water scarcity impacting cooling systems
- Storms and adverse winds affecting open or external infrastructure
- Power supply disruption linked to environmental events or a deviation of expected power source

Key Requirements

- **Risk Assessment**
 - Climate-related physical risks shall be assessed:
 - During site selection (new builds)
 - Environmental impacts assessments (New Builds)
 - Periodically (existing sites), where applicable
 - Assessments should align with **TCFD recommendations**.
- **Resilience Measures**
 - Implementation of:
 - Flood defenses, considerations and site elevation controls
 - Redundant cooling systems design (N+1 or greater)
 - Load management between power streams
 - Backup power resilience, with emergency controls and preparedness
- **Scenario Planning**
 - Climate scenarios (1.5°C, 2°C, 4°C warming) shall be considered in long-term planning.
 - Seasonal effects

- **Incident Management**
 - Physical climate incidents shall be:
 - Logged and investigated and reviewed for further investment and residual controls
 - Incorporated into business continuity planning
 - Communication and consideration if full impact
- **Integration with ICT and Operational Risk**
 - Physical risks must be incorporated into:
 - Enterprise Risk Management (ERM) and investors
 - ICT Risk Management frameworks applicable ISO31000:2018
 - Site-level operational risk registers and review
- **Monitoring & Reporting**
- Annual review of:
 - Climate risk exposure and scope
 - Mitigation effectiveness
- Reporting to ELT and inclusion in ESG disclosures assurance from 3rd party

Roles	Responsibilities
Compliance/ESG Function	Policy oversight and implementation, reporting and regulatory alignment
Engineering/Operations	Implementation, monitoring and maintenance of water, energy related to resilience controls.
Procurement	Supplier alignment with GHG and sustainability requirements
ELT/Investors	Approval, authorisations of targets, strategy and scope of risk

Closed Loop water management

The organisation shall continue to implement by design and factor in to minimise potable water consumption and environmental discharge through the implementation of **closed loop and water-efficient cooling systems**.

1. Key Requirements

- **Closed Loop Systems**
 - Cooling systems shall be designed, prioritised, and maintained as **closed loop systems** where technically feasible, but not limited to an legacy locations.
 - Water recirculation must be maximised to reduce abstraction from municipal or natural sources. As part of design and environmental commitments through the VIRTUS design model
- **Water Efficiency Controls**
 - Target reductions in **Water Usage Effectiveness (WUE)** shall be defined and monitored at each location

- Use of alternative water sources (e.g., greywater, harvested rainwater, recycled water) shall be assessed and considered as a last resort inline and working with local and regulatory authorities
- Minimize usage by using a free cooling element as frequently as possible
- **Monitoring and Reporting**
 - Continuous monitoring of:
 - Water inflows (m³)
 - Onsite water abstraction submissions (LONDON2)
 - Water usage and levels (LONDON2)
 - Water usage for treatment and utilities
 - Monthly reporting and annual review of water efficiency performance.
- **Compliance**
 - All water abstraction and discharge must comply with **local environmental permits and regulatory requirements** including abstraction licenses with 6 yearly renewals and annual reporting
 - Annual monitoring, reporting and reducing as far as reasonably practicable



Interested and Affected Parties:

There are a number of stakeholders and interested parties associated with the services offered. Feedback from these parties will be sought where possible to ensure compliance is met and remains appropriate & effective to VIRTUS' business needs.

Interested Party	Stake/Interest	Potential Feedback/Input
Internal Users/ Staff	• Compliance with policies and procedures • Disciplinary action related to non-conformance • Protection of their personal data (People Team) • Implications to regulations • Professional development, training and awareness • Involvement in policy, process and control development • Decisive decision making • Provision of the tools, knowledge and training required to assume their responsibilities • Clear and accurate job descriptions, responsibilities and accountabilities • Safe working conditions and processes (including risks arising from epidemics and pandemics)	• Staff training/forum feedback • Exceptions to policies and procedures • Reporting of incidents, events and weaknesses • Awareness communications • Internal and external audit findings
Customers	• Security and achievement of contracted services • Confidence in our operational and business continuity processes • 100% uptime of data centre power • Responsive, accurate communications from VIRTUS • Strategic and future planning • Certification and/or conformance to industry-best standards and practices • Compliance to applicable regulation • Safe working conditions (including risks arising from epidemics and pandemics) • Competitive service pricing	• Security requirements within contracts • Customer feedback/complaints • Incident management • 24-hour service management centre

Suppliers / Partners	• Protection of personal data	
	• Service provision critical to our businesses • Holistic compliance to applicable regulation	• Reported incidents • Service agreements • Service review meetings and reporting • Key performance indicators
The Board / Senior Management	• Compliance with regulation, legislation and contractual/SLA obligations • Competitive advantage • Effective power & capacity management • Top-down decision making, policy development and business controls • Accountable party • 100% uptime of data centre power • Planned, tried and tested business continuity management • Reduction of the likelihood of major accidents and injuries – Preservation of duty of care • Risk-based information to drive business decisions	• Applicable legislation/ changes to legislation • Planned business changes impacting service delivery • Incident management
Investors	• Compliant management of the business • Business growth and expected returns • Risk-based information to drive business decisions	• Investor meetings • Board meetings
Regulators (Customers) (EA) (Local Council) (HSE)	• Compliance with regulation, legislation and contractual obligations • Mandatory adherence to permits and licences • Provide on time and transparent information when reporting • Provide resources to auditing • Access to relevant information/data • Reduction of the likelihood of major accidents and injuries	• Applicable legislation/ changes to legislation/ Code of practice • Site visitations • Notification
Government	• Compliant reporting	• Notifications

	• Access to relevant information/data • Provide resources for investigatory powers • Reduction of the likelihood of major accidents and injuries	• Requests for information
Neighbours / Community	• Activities that could be considered a Nuisance (noise/smoke)	• Neighbour/Community feedback/complaints • Notifications from local councils
Landlord	• Compliance with contractual obligations	• Planned contractual changes impacting upon compliance requirements
Certification bodies	• Compliance with contractual obligations • Compliance with standard requirements	• Planned contractual changes impacting upon compliance requirements • Changes to Standard(s) impacting upon compliance requirements

Scope:

For the purposes of certification within VIRTUS Data Centres, the boundaries of this policy and the scope of certification is:

BS EN ISO 9001:2015	The design, build and ongoing operation of mission critical Tier III data centre facilities.
BS EN ISO 14001:2015	The design, build and ongoing operation of mission critical Tier III data centre facilities.
BS EN ISO 50001:2018	The Management of energy relating to the design, build and ongoing operation of mission critical Tier III London Data Centres as follows; LONDON1, LONDON2, LONDON3/4, LONDON5, LONDON6, LONDON7, LONDON8 LONDON9, LONDON10, LONDON11 and Head Office, London in accordance with the EnMS and applicable energy legislation.
ISO/IEC 27001:2022	Information security management for the design, build and ongoing operations of mission critical Tier III data centre facilities. In accordance with the statement of applicability issue 5.4.
ISO/IEC 20000-1:2018	The Service management system of VIRTUS Holdco Limited (trading as VIRTUS Data Centres) supporting the provision of the build and ongoing operation of data centre facilities consisting of retail and wholesale colocation, supporting cloud and high-density computing models to customers from LONDON1 – Enfield, LONDON2 – Hayes, LONDON3/4, LONDON9, LONDON10, LONDON11 – Slough, LONDON5,

	LONDON6, LONDON7, LONDON8– Stockley Park in accordance with Service Catalogue.
BS EN ISO 22301:2019	The business continuity management system relating to the ongoing operation of mission critical, Tier III London data centre facilities in conformance with the Compliance Policy and business continuity plans.
BS ISO 45001:2018	The occupational health & safety management system relating to the ongoing operation of mission critical, Tier III London data centre facilities in accordance with applicable legislation and the VIRTUS occupational health & safety policy.

These activities are carried out from:

Site Name	Location Type
VIRTUS Headquarters (LONDON)	Head Office
LONDON1 (Enfield)	Data Centre
LONDON2 (Hayes)	Data Centre
LONDON3/4 (Slough)	Data Centre
LONDON5 (Stockley Park)	Data Centre
LONDON6 (Stockley Park)	Data Centre
LONDON7 (Stockley Park) LONDON7 South (Stockley Park)	Data Centre
LONDON8 (Stockley Park)	Data Centre
LONDON9 (Stockley Park)	Data Centre
LONDON10 (Slough)	Data Centre
LONDON11 (Slough)	Data Centre
LONDON12 (Slough)	Data Centre
LONDON14 (Stockley Park)	Data Centre
LONDON15 (Saunderton)	Data Centre
LONDON16 (Saunderton)	Data Centre
LONDON17 (Saunderton)	Data Centre
LONDON18 (Saunderton)	Data Centre

This policy applies to all individuals working at all levels, including Senior Management, Officers, Directors, Employees (whether permanent, fixed term or temporary), Trainees, Interns, Agents, Sponsors, or any other person associated with VIRTUS (involved third parties). This policy should be communicated to key Consultants, Contractors, Suppliers, Business Partners and other similar involved third parties engaged by

VIRTUS, and a commitment obtained from them that they will both comply with it themselves and require any sub-contractors to comply with an equivalent policy.

Responsibilities:

All Employees are responsible for building service delivery, service management, quality, energy & environmental and information security considerations into their day to day activities at VIRTUS. The company is responsible for maintaining management systems, communicating the requirements and policing adherence to its protocols. This is achieved through designating specific roles and responsibilities in related manuals, such as the VIRTUS Operations Manual. The Executive leadership team of the company are ultimately responsible for legal implications.

Roles, responsibilities, and accountabilities are further detailed to individual and process level to include, where necessary, specific roles directly pertaining to service delivery, service management, quality, energy & environmental and information security management.

Directors and Managers shall ensure that any third-party contractors are adequately qualified, are aware of our policies and processes, the need to deliver agreed services and conducting appointed activities legally, ethically and in accordance with agreements.

Each Employee has a duty to comply with our policies & processes, in order to determine and where possible, exceed customer expectations, and to work in a manner (within their areas of responsibility):

- To prevent pollution and promote energy & environmental considerations



- That reduces the risk of breaches of information
- That promotes continual service delivery and customer satisfaction, including business continuity planning
- To continually improve processes and drive continual improvement throughout the company
- That has the company's best interests in mind.

This Policy will be available at all sites and offices and to the general public via the VIRTUS website. This Policy will be reviewed & approved on an annual basis by the ELT or sooner if required.

VIRTUS Data Centres ensures that internal and external issues relevant to the provision of services, energy & environmental, information security, our strategic direction and to maintaining compliance are captured, evaluated and mitigated through a Risk Management System compliant with the requirements of BS ISO31000:2018 Risk Management.

