

# Vertica Accelerator Security Statement

This Security Statement is aimed at providing you with information about the information security management system implemented by Vertica, with applicability to Vertica Accelerator.

## Information Security Management System (ISMS)

Vertica is committed to protecting our customer's information. To achieve this goal, Vertica has implemented an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2013.

The overarching framework that overlays the Vertica ISMS is the Micro Focus Information Security Policy Framework (ISPF), the Micro Focus set of information security policies. It consists of a set of security requirements to protect company and customer information.

## Vertica Accelerator at a Glance:

### Customer Empowerment:

- Vertica Accelerator is housed in Amazon Web Services (AWS). It runs in your AWS account.
- This approach allows you to keep all the data and compute resources on your own secure cloud and maintain preferred pricing and flexibility with AWS.
- We require cross-account roles in your AWS account to deploy and administer Vertica Accelerator, but we use the principles of least-privilege in the construction of these roles.

### Cloud-Native Architecture:

- Vertica Accelerator delivers high-performance and scalable analytics as well as end-to-end, in-database machine learning to organizations that require the right level of resourcing, management, and control for each analytical use case – all built on the proven cloud-native architecture of Vertica.

### Advanced Analytics as a Service:

- Vertica Accelerator offers organizations much greater transparency and control – control of

their environment, control over tuning their queries, ownership of their data – all while relying on a field-proven, cloud-optimized architecture that delivers the highest levels of performance at extreme scale with forecastable and transparent pricing,

Vertica is a Micro Focus Product Group. Micro Focus helps 40,000 companies worldwide run and transform, including 98 of the Fortune 100.

Micro Focus produces the world's leading security products. The combined information security personnel of Vertica and Micro Focus number more than 400, providing our customers with unparalleled security experience and expertise.

For more information see the [Micro Focus Product Security Page](#).

## Information Security Policies

Vertica has implemented a set of policies for information security that are defined and approved by management, published, and communicated to employees and relevant external parties.

## Organization of Information Security

Vertica has defined and allocated information security responsibilities with appropriate segregation of duties.

## Human Resource Security

Vertica performs background verifications on all personnel and requires acknowledgement of their responsibilities for information security.

Vertica personnel receive security education and training and regular updates in organizational policies and procedures, as relevant for their job functions.



## Asset Management

Vertica maintains an asset inventory with assigned owners. Vertica personnel are trained in the acceptable use of assets associated with information and information processing facilities.

## Access Control

Vertica has established access control policy and procedures that control user registration and de-registration. Access to information and application system functions are restricted in accordance with the access control policy.

## Cryptography

Policies and procedures on the use of cryptographic controls for protection of information have been developed and implemented. A key management system is utilized to guide the use, protection, and lifecycle of cryptographic keys.

Contact us at:  
[www.vertica.com](http://www.vertica.com)

Like what you read? Share it.



### Physical and Environmental Security

Vertica corporate offices are protected by industry-leading physical and environmental controls.

### Operations Security

Vertica has documented playbooks that guide operations. Separate development, testing, and operational environments are utilized.

There are established controls for backup, change management, logging, malware, and vulnerability management.

### Communications Security

Networks are managed and controlled to protect information in systems and applications.

### System Acquisition, Development, and Maintenance

Information security-related requirements are specified for new information systems or enhancements to existing information systems.

Vertica follows a secure development lifecycle that introduces security and privacy considerations throughout all phases of development.

### Supplier Relationships

Information security requirements for mitigating risks associated with supplier's access to the organization's assets are agreed to with the supplier and documented.

### Information Security Incident Management

Vertica has an established incident management process to ensure a quick, effective, and orderly response to information security incidents.

### Information Security Aspects of Business Continuity Management

Vertica has a documented business continuity and disaster recovery plan. Redundant assets and data replication have been set up to ensure continuity and recovery.

### Compliance

All relevant legislative, statutory, regulatory, and contractual requirements are explicitly identified, documented, and kept up to date for each information system and the organization.

Controls for the privacy and protection of personally

identifiable information are implemented.

Vertica is intent on ensuring our information security management system remains cutting edge. To this end, we have undertaken an ISO 27001 audit of our information security management system. We expect to be certified by January 2022.

The Vertica ISMS also assimilates the acquired Full 360 ISMS which has an [active ISO 27001 certification](#), valid thru June 2024.

