Vertica Accelerator 보안 정책

본 보안 정책은 Vertica 에서 구현한 정보 보안 관리 시스템에 대한 정보를 Vertica Accelerator 에 적용할 수 있도록 제공하기 위한 것입니다.

ISMS(Information Security Management System)

Vertica 는 고객의 정보를 보호하기 위해 최선을 다하고 있습니다. 이 목표를 달성하기 위해 Vertica 는 ISO/IEC 27001:2013 에 따라 ISMS(Information Security Management System)를 구현했습니다.

Vertica ISMS 와 오버레이되는 가장 중요한 프레임워크는 Micro Focus 정보 보안 정책 집합인 Micro Focus ISPF(Information Security Policy Framework)입니다. 이것은 회사 및 고객 정보를 보호하기 위한 보안 요구 사항 집합으로 구성됩니다.

Vertica Accelerator 한눈에 보기:

고객 강화:

- Vertica Accelerator 는 AWS(Amazon Web Services) 안에 있습니다. AWS 계정 내에서 실행됩니다.
- 이 접근 방식은 모든 데이터 및 컴퓨팅 리소스를 자사 보안 클라우드에 보관하고 AWS 의 기본 가격 및 유연성을 유지할 수 있게 해줍니다.
- Vertica Accelerator 를 배포하고 관리하려면 AWS 계정에서 교차 계정 역할이 필요하지만, 이러한 역할을 구성할 때는 최소 권한 원칙이 사용됩니다.

클라우드 네이티브 아키텍처:

- Vertica Accelerator 는 고성능의 확장 가능한 분석뿐만 아니라 데이터베이스 내 머신 러닝을 각 분석 사용 사례에 맞는 적절한 수준의 리소스 조달, 관리 및 제어가 필요한 조직에 제공합니다. 이 모든 것은 Vertica 의 검증된 클라우드 네이티브 아키텍처를 기반으로 합니다.

Advanced Analytics as a Service:

- Vertica Accelerator 는 조직의 투명성과 통제력(환경 제어, 쿼리 조정 제어, 데이터 소유권 등)을 높입니다. 이 모든 것은 예측 가능하고 투명한 가격으로 매우 유연하게 확장할 수 있는 최고의 성능을 제공하는 현장에서 검증된 클라우드 최적화 아키텍처 덕분입니다.

Vertica 는 Micro Focus 제품 그룹입니다. Micro Focus 는 Fortune 100 기업 중 98 개를 포함하여 전 세계 40,000 개 기업의 운영과 혁신에 도움을 줍니다.

Micro Focus 는 세계 최고의 보안 제품을 생산합니다. Vertica 와 Micro Focus 의 정보 보안 인력을 모두 합치면 400 명이 넘으며, 타의 추종을 불허하는 보안 경험과 전문성을 고객에게 제공합니다.

자세한 내용은 Micro Focus 제품 보안 페이지를 참조하세요.

정보 보안 정책

Vertica 는 경영진이 결정 및 승인한 후 공표되고 직원 및 관련 외부 당사자에게 전달되는 일련의 정보 보안 정책을 구현했습니다.

정보 보안 조직

Vertica 는 적절한 업무 분리를 통해 정보 보안 책임을 규정하고 할당했습니다.

인적 자원 보안

Vertica 는 모든 인력에 대해 백그라운드 검증을 수행하며, 정보 보안에 대해 각자가 책임을 맡을 것을 요구합니다.

Vertica 직원은 자신의 직무와 관련된 조직 정책 및 절차에 대한 보안 교육과 정기적인 업데이트를 받습니다.

자산 관리

Vertica 는 자산 재고를 할당된 소유자와 함께 관리합니다. Vertica 직원은 정보 및 정보처리시설과 관련된 자산을 적절히 사용하는 것에 대한 교육을 받았습니다.

액세스 제어

Vertica 는 사용자 등록 및 해지를 제어하는 액세스 제어 정책 및 절차를 수립했습니다. 정보 및 애플리케이션 시스템 기능에 대한 액세스는 액세스 제어 정책에 따라 제한됩니다.

암호화

정보 보호를 위해 암호화 컨트롤을 사용하는 것에 대한 정책 및 절차가 개발되고 구현되었습니다. 키 관리 시스템이 암호화 키의 사용, 보호 및 라이프사이클을 안내하는 데 사용됩니다.

연락처:
www.vertica.com

글이 도움이 되었다면 공유해주세요.

물리적 및 환경적 보안

Vertica 기업 사무실은 업계 최고의 물리적 및 환경적 제어로 보호됩니다.

운영 보안

Vertica 는 운영을 안내하는 플레이북을 문서화했습니다. 별도의 개발, 테스트 및 운영 환경이 활용됩니다.

백업, 변경 관리, 로깅, 맬웨어 및 취약점 관리를 위한 컨트롤이 설정되어 있습니다.

통신 보안

시스템 및 애플리케이션의 정보를 보호하기 위해 네트워크가 관리되고 제어됩니다.

시스템 구입, 개발 및 유지 보수

새로운 정보 시스템 또는 기존 정보 시스템 개선을 위한 정보 보안 관련 요구 사항이 명시되어 있습니다.

Vertica 는 모든 개발 단계에서 보안 및 개인정보보호 고려 사항을 도입하는 안전한 개발 라이프사이클을 따릅니다.

공급업체 관계

공급업체가 조직 자산에 액세스하는 것과 관련된 리스크를 완화하기 위한 정보 보안 요구 사항이 공급업체와 합의되어 문서화됩니다.

정보 보안 인시던트 관리

Vertica 는 정보 보안 인시던트에 신속하고 효과적이며 질서 있게 대응하기 위한 인시던트 관리 프로세스를 수립했습니다.

비즈니스 연속성 관리의 정보 보안 측면

Vertica 는 문서화된 비즈니스 연속성 및 재해 복구 계획을 가지고 있습니다. 연속성과 복구를 보장하기 위해 중복 자산과 데이터 복제가 설정되었습니다.

규정 준수

모든 관련 법률, 법규, 규제 및 계약상의 요구 사항은 각 정보 시스템과 조직에 대해 명시적으로 식별되고, 문서화되고, 최신 상태로 유지됩니다.

개인 식별 가능 정보의 개인정보보호를 위한 제어가 구현되어 있습니다.

Vertica 는 정보 보안 관리 시스템을 최첨단으로 유지하기 위해 노력하고 있습니다. 이를 위해 정보 보안 관리 시스템에 대한 ISO 27001 감사를 실시했습니다. 2022 년 1 월까지 인증을 받을 수 있을 것으로 예상합니다.

또한 2024 년 6 월까지 유효 ISO 27001 인증을 보유한 Full 360 ISMS 을 인수했으며 이를 Vertica ISMS 에 통합했습니다.