

IBM 클라우드 서비스 명세

IBM Digital Data Exchange

다음은 귀하의 주문을 위한 서비스 명세입니다.

1. 클라우드 서비스

기본 오퍼링과 선택적 기능을 포함하는 이 클라우드 서비스 오퍼링은 주문 서류에서 선택되며 아래에 기술되어 있습니다. 주문 서류는 제공되는 견적서와 POE(Proof of Entitlement)로 구성되며, IBM은 클라우드 서비스의 시작일과 기간을 확인하는 POE를 청구를 시작하는 시점에 귀하에 제공합니다.

1.1 IBM Digital Data Exchange

IBM Digital Data Exchange는 웹 사이트 및 모바일 페이지 태그를 구성하고 배치하기 위한 하나의 인터페이스를 제공하는 솔루션입니다.

IBM Digital Data Exchange를 사용하여 귀하의 웹 또는 모바일 사이트에 배치된 IBM 태그와 IBM 비즈니스 파트너 태그를 관리할 수 있습니다. IBM Digital Data Exchange 사용자 인터페이스는 태그 실행을 결정하는 일련의 규칙을 바탕으로 태깅 프로세스, 사용자에게 페이지 태그와 페이지 그룹을 정의하는 기능 부여에 대한 직접적인 통제력을 제공합니다. 일단 IBM Digital Data Exchange를 구입하면, 여러 환경에 대한 현재 또는 과거에 적용한 IBM 태그, IBM 비즈니스 파트너 태그 및 사용자 정의 JavaScript 또는 고유 코드(proprietary code)를 관리할 수 있습니다.

2. 보안 설명

2.1 보안 정책

IBM은 IBM 직원에게 발표하고 전달되는 개인 정보 보호와 보안 정책을 운용합니다. IBM은 IBM 데이터 센터를 지원하는 전세계 개인 직원에게 개인 정보 보호 및 보안 교육을 실시하도록 요청하며 정보 보안을 담당하는 보안 팀을 운영합니다. IBM 보안 정책 및 기준에 대한 검토와 평가는 연단위로 이루어집니다. IBM 보안 사고는 종합적인 사고 대응 절차에 따라 처리됩니다.

2.2 접근 권한 통제

IBM은 고객 데이터에 대한 논리적 분리상태를 유지합니다. 고객 데이터는 그 클라이언트 소유의 스키마에 있게되며, 저장되며 클라우드 서비스 또는 클라이언트 지정 데이터 export를 통해 접근가능하도록 디자인됩니다. 네트워크 인프라스트럭처 내, IBM 데이터 센터 내 개인들의 워크스테이션 또는 IBM 데이터센터 내 고객 데이터로 수행되는 하드웨어, 소프트웨어, 액세스 로그, 읽기 전용 액세스, 암호화 제어는 컴퓨터 바이러스와 알려진 유해 코드의 확산과 실행 가능성을 줄이기 위해서 활용됩니다. IBM은 클라이언트 시스템 액세스시에 다중 요소 인증(multi-factor authentication)과 암호화된 VPN 터널 기술을 사용합니다. 접근 권한은 클라우드 서비스 및 제 3 자 데이터센터에 소재한 관련 하드웨어, 소프트웨어 인프라스트럭처를 관리와 운용을 하기 위하여 접근 권한이 필요한 개인들에게만 부여됩니다. IBM은 AES 암호화 알고리즘 옵션이 포함된 WPA2를 통해 암호화되는 WIFI(802.11) 네트워크 트래픽을 사용하며, 고객 데이터가 저장된 시스템 접근 시 non-broadcast SSID와 서버와 엔드 디바이스 간 상호 인증을 제공합니다.

2.3 서비스 무결성과 가용성

운영 체제 자원(OSR)과 애플리케이션 소프트웨어에 대한 수정은 IBM 변경 관리 프로세스에 의하도록 합니다. 네트워크 인프라스트럭처 내에서 IBM 데이터 센터 관련 작업을 수행하거나 IBM 데이터 센터에서 고객 데이터 관련 작업을 수행하는 개인의 워크스테이션의 경우 하드웨어, 소프트웨어, 액세스 로그, 읽기 전용 액세스, 암호화 제어를 사용하여 컴퓨터 바이러스 및 알려진 유해 코드의 확산과 실행을 줄이기 위해 노력합니다. IBM은 표준 SSL (https) 연결을 통한 over-the-network 암호화를 사용하며, IBM 인프라스트럭처는 방화벽, 침입 예방, 안티 멀웨어 기술을 포함한 end-to-end의 기술적인 솔루션을 활용합니다. 잠재적인 시스템 보안 취약점을 감지하고, 해결하기 위하여, TCP/IP(Transmission Control Protocols/Internet Protocol) 취약성 스캐닝은 권한있는 관리자에 의하여 정기적으로 실시됩니다. IBM 웨어하우스 데이터는 IBM 데이터 센터의 2 차 스토리지에 복사되며 3 차 아카이브(테이프)는 제 3 자 오프사이트 재해 복구 시설에 저장을 위해 암호화되고 복제됩니다.

2.4 활동 로깅

IBM 은 로깅 활동이 가능하도록 구성된 시스템, 애플리케이션, 데이터 저장소, 미들웨어 및 네트워크 인프라스트럭처 디바이스의 활동 로그를 유지 관리합니다. IBM 은 기록을 위하여 다음의 로그를 유지합니다. i) 성공 및 실패한 로그인 액세스 시도, ii) 외부 장소에서 인프라스트럭처에 대한 액세스 권한을 얻는 데 성공 및 실패한 시도, iii) OSR 에 대한 업데이트 액세스 시도 및 iv) 시스템 또는 보안 관리자 권한으로 수행된 활동.

2.5 물리적 보안

IBM 은 IBM 내와 제 3 자 제공 데이터센터에 권한을 부여받은 사람에 대해서만 접근하도록 합니다. IBM 클라우드 서비스 환경은 24 x 7 보안 담당, 유인 보안, 비디오 감시뿐만 아니라 물리적 접근통제 대한 고유 코드 및 생체 인식 스캔을 채용한 다중 요소 인증(multiple-factor authentication)을 포함합니다. IBM 은 고객 데이터가 포함된 매체가 권한없이 열람, 복사, 변경 또는 제거하는 것은 금지합니다. 고객 데이터가 저장된 이동식 매체(섬 드라이브, CD, DVD 포함)는 최소 256 비트 AES(또는 그와 동등)를 사용하여 암호화됩니다. 접근 권한 민감 정보 또는 고객 데이터에 대한 접근 권한이 필요한 경우, IBM 지급 랩탑과 워크스테이션은 전체 디스크 암호화(PGP)가 요구됩니다. IBM 은 고객 데이터가 포함된 이동식 매체와 모든 모바일 디바이스(예: 디스크, USB 드라이브, DVD, 백업 테이프, 프린터, 랩탑)는 폐기 또는 재사용하기 전에 판독이나 재구성이 불가능하도록 조치하여야 합니다. 폐지는 판독이 불가능하도록 보안 및 기밀 보호 방식으로 파쇄하여 처리합니다.

2.6 법규의 준수

IBM 은 IBM 개인정보 보호정책이 미국 상무부의 Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement 에 부합하는지 연단위로 확인합니다. 산업 표준 감사 SSAE 16 타입(기존의 SAS 70) 또는 그와 동등한 감사가 매년 프로덕션 데이터 센터에서 수행됩니다. IBM 은 IBM 비즈니스 요건을 준수하기 위해 보안 및 개인 정보 보호 관련 활동을 검토합니다. IBM 은 정기적인 평가와 감사를 통해 정보 보안 정책을 준수하는지 여부를 확인합니다. 보안정책은 보안 감사, 정기적인 보안 패치 애플리케이션 적용, 비밀번호 관리와 통제를 규정하고 있습니다. IBM 직원과 공급업체 직원을 대상으로 보안 인식 교육을 매년 실시합니다. 업무 목표, 윤리 강령 기밀 보호 의무, IBM 의 보안 의무를 이행하여야 하는 책임을 매년 직원들에게 숙지시킵니다.

3. 서비스 레벨 목표 (Service Level Objectives, "SLO")

IBM 은 99%의 IBM SaaS 가용성을 고객에게 제공하도록 노력합니다. SLO 는 계약상의 약속이나 의무는 아니며, IBM 고객 지원 팀의 절차, 기술 및 담당자를 통해 달성 또는 초과하고자 노력하는 목표입니다.

4. 권한 부여 및 대금 청구 정보

4.1 과금 체계

클라우드 서비스는 주문 서류에 지정된 바와 같이 다음 중 하나의 과금 체계 하에서 제공됩니다.

- a. MSC(Million Server Calls)는 클라우드 서비스 구입 시 사용되는 측정 단위입니다. Server Call 은하나의 Entity ID 로 트래킹되는 방문자에 의해 시작된 태깅된 이벤트의 결과로 클라우드 서비스로 전달되고, 처리된 데이터를 의미합니다. 서로 다른 Entity ID 에서 처리된 하나의 Server Call 은 각각의 고유 법인 ID 에 대한 고유한 Server Call 로 계산됩니다. 하나의 Entity ID 는 하나 이상의 귀하 웹 사이트에서 처리된 데이터가 포함되어 있는 클라우드 서비스의 데이터에 대한 액세스 권한을 구분하거나 제어합니다. 각 MSC 권한은 1 MSC(Million Server Calls)를 의미합니다. 주문 서류에 명시된 측정 기간 동안 처리된 Server Call 수를 포괄할 수 있는 충분한 MSC 권한을 취득해야 합니다.

4.2 대금 및 청구

클라우드 서비스에 대해 지불하는 대금은 주문 서류에 명시됩니다.

5. 기간 및 갱신 옵션

5.1 기간

클라우드 서비스의 기간은 IBM 이 귀하가 클라우드 서비스 부분에 대해 액세스 권한을 가진다고 귀하에게 통지한 날로서 주문 서류에 명기된 날부터 시작됩니다. 해당 기간의 정확한 시작 날짜와 종료 날짜는 주문 서류의 POE 부분에 명시됩니다. 귀하는 IBM 또는 IBM 비즈니스 파트너와의 계약을 통해 해당 기간 동안 클라우드 서비스의 사용 레벨을 증가시킬 수 있습니다. IBM 은 상향 조정된 사용 레벨을 주문 서류에 명시합니다.

5.2 클라우드 서비스 기간 갱신 옵션

귀하의 주문 서류에는 다음 중 하나를 선택하여 클라우드 서비스의 기간 종료 시 갱신 여부를 명시할 수 있습니다.

5.2.1 자동 갱신

주문 서류에서 자동 갱신으로 명시한 경우 귀하는 주문 서류에 지정된 기간 만료일보다 최소 90 일 이전 서면 요청을 통해 클라우드 서비스를 해지할 수 있습니다. IBM 또는 IBM 비즈니스 파트너가 만료일까지 그러한 해지 통지를 받지 못한 경우 만료 기간은 1 년 또는 POE 에 명시된 최초 기간과 동일한 기간만큼 자동으로 갱신됩니다.

5.2.2 연속적 청구

주문 서류에서 연속적 청구로 명시한 경우 귀하는 계속해서 클라우드 서비스에 대한 액세스 권한을 가지며 연속적 기준에 따라 클라우드 서비스의 사용 대금이 청구됩니다. 클라우드 서비스의 사용을 중단하고 연속적 청구 절차를 중지하려면, 클라우드 서비스의 취소를 요청하는 서면 통지가 90 일 전에 IBM 이나 IBM 비즈니스 파트너에게 제공해야 합니다. 귀하의 액세스가 취소되면 취소가 발효된 해당 월의 미지불된 액세스 대금이 귀하에게 청구됩니다.

5.2.3 직접 갱신

주문 서류에서 갱신 유형을 "종료"로 지정한 경우에는 기간이 만료되면 클라우드 서비스가 종료되며 클라우드 서비스에 대한 액세스 권한은 소멸됩니다. 종료 날짜 이후에도 클라우드 서비스를 계속 사용하려면 IBM 영업 담당자나 IBM 비즈니스 파트너에게 새로운 등록 기간을 구매하는 주문 서류를 접수해야 합니다.

6. 기술 지원

기술 지원은 등록 기간 동안 IBM SaaS 오퍼링과 인에이블링 소프트웨어에 대해 제공됩니다. 기술 지원은 IBM SaaS 에 포함되며 별도의 오퍼링으로 제공되지 않습니다.

기술 지원 정보는 다음 URL 에서 확인할 수 있습니다. http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

7. 인에이블링 소프트웨어(Enabling Software)

- a. 본 클라우드 서비스 오퍼링에는 인에이블링 소프트웨어가 포함되어 있을 수 있습니다. 귀하는 클라우드 서비스 기간에 클라우드 서비스 이용과 관련해서만 인에이블링 소프트웨어를 사용할 수 있습니다. 인에이블링 소프트웨어에 샘플 코드가 포함되어 있으면 샘플 코드의 2 차적 저작물을 작성하고 본 권한에 따라 2 차적 저작물을 사용할 수 있는 권리가 귀하에게 추가로 부여됩니다. 인에이블링 소프트웨어는 SLA(있는 경우)에 의거하여 클라우드 서비스의 구성요소로 제공되며 "현상태대로(AS IS)" 제공됩니다.

8. 추가 정보

8.1 권한 상세 정보

IBM Digital Data Exchange 의 등록료에는 다음이 포함됩니다.

- a. IBM Digital Data Exchange 의 단일 인스턴스를 제공합니다.
- b. IBM Digital Data Exchange 의 초기 온보딩을 위해 원격으로 제공되는 최대 5 시간의 구현 서비스에 대한 표준 인에이블먼트. 서비스는 제공된 시간을 모두 사용했는지 여부에 관계 없이 IBM 이 클라우드 서비스에 대한 액세스를 허용한다고 통지한 날 이후 90 일에 만료됩니다.

8.2 개인정보 보호 주의사항 및 정책

귀하는 (i) 귀하 웹 사이트 이용 약관 및 개인정보 보호정책에 관한 명확하고 눈에 잘 띄는 링크(IBM(<http://www.ibm.com/software/marketing-solutions/privacy/index.html>)) 및 귀하의 정보 수집과 정보 이용 규정 관련 링크 포함)를 제공하고 (ii) 귀하를 대신하여 IBM 이 방문자의 컴퓨터에 쿠키와 clear gifs/웹 비콘을 배치한다는 알림을 관련 기술의 목적 및 용도에 대한 설명과 함께 제공하며 (iii) 법률에서 요구하는 경우, 귀하나 귀하를 대신하는 IBM 이 웹 사이트 방문자의 디바이스에 쿠키와 clear gifs/웹 비콘을 배치하기 전에 웹 사이트 방문자의 동의를 얻도록 하여야 합니다.

귀하는 IBM 이 클라우드 서비스의 정상적인 운영과 지원 활동의 일부로서, 트래킹또는 기타 기술을 사용하여 클라우드 서비스 사용과 관련된 개인 정보를 귀하(귀하의 직원과 하도급자)로부터 수집할 수 있다는 것을 인정하고 이에 동의합니다. IBM 은 사용자 경험을 개선하거나 상호작용을 조정할 목적으로 클라우드 서비스의 효율성에 대한 통계와 정보를 수집합니다. 귀하는 IBM, 기타 IBM 회사 및 하도급자 내부에서, 그리고 IBM 및 IBM 하도급자가 비즈니스를 수행하는 어디서나, 관련 법률을 준수하면서, 상기의 목적으로 수집된 개인 정보를 IBM 이 처리하기 위해 필요한 동의를 이미 획득했거나 획득할 것임을 확인합니다. IBM 은 수집된 개인 정보에 접근하거나 갱신하거나 정정하거나 삭제하고자 하는 고객 직원과 하도급자의 요청을 수용합니다.

8.3 사업장 위치의 의제

해당하는 경우, 세금은 귀하가 클라우드 서비스의 혜택이 제공되는 것으로 식별한 사업장을 기준으로 부과됩니다. 추가 정보를 제공하지 않는 한, IBM 은 클라우드 서비스 주문 시 주사업장으로 제출한 비즈니스 주소에 따라 세금을 적용합니다. 귀하는 이러한 정보를 최신 상태로 유지하고 변경사항이 있는 경우 IBM 에 제공해야 할 책임이 있습니다.