대 외 비 - 영구
지경정 22-01
보안위원회
’22. 1. 17

데이터베이스 통제지침

’22. 1. 17.
보안위원회

보고서의 다음 사항을 개선합시다	
주요 체크 항목	판단
1. 메모/이메일/구두보고로 대체 가능?	Yes (No)
2. 장수를 축소할 여지가 있는가?	Yes (No)
3. 대면 보고를 꼭 해야 했는가?	(Yes) No
4. 결과(So What)은 있는가?	(Yes) No
5. 근거(Fact)는 적절한가?	(Yes) No
6. 실행계획(Next Step)은 있는가?	(Yes) No
7. 헤드메세지와 내용은 일치하는가?	(Yes) No
8. 중앙에 집중/압축(시선집중) 되어 있는가?	(Yes) No
9. 그래프/도표를 적절히 사용했는가?	(Yes) No
10. 페이지/단위 표시는 되어 있는가?	(Yes) No

문서 변경 이력

버전	승인일자	기안자	내 용	비 고
1.0	‘19.9.23	주진국	최초 작성	
1.1	‘22.01.17	주진국	GS리테일 / GS홈쇼핑 합병에 따른 개정	

목 차

문서번호	업무구분	문서제목	최초시행	개정일시
1조 ~ 3조	제1장 개요	데이터베이스 통제지침	'19. 9. 23.	'22. 1. 17.

제1장 개요

제1조 목적

본 지침은 GS리테일(이하 '회사'라고 한다)의 데이터베이스 데이터베이스 무결성에 대한 지침 및 데이터베이스 접근제어, 데이터베이스 암호화, 데이터베이스 감사 등에 대하여 DBA(Database Administrator) 및 정보보안 책임자 등 관련 담당자가 시행하여야 할 지침을 정함에 그 목적이 있다.

제2조 적용 대상

본 지침은 회사에서 규정하고 있는 데이터베이스 자산에 적용되며 아래 내용을 포함한다.

① 정형 데이터
② 비정형 데이터
③ 데이터베이스 서버
④ 데이터베이스 계정
⑤ 데이터베이스 암호화 키
⑥ 데이터베이스 소프트웨어

제3조 용어 정의

① 가용성(availability) : 인가된 개체(entity), 사용자가 정보시스템에 접근하여 정보를 항상 사용할 수 있게 하는 특성이다.
② 감사(audit) : 시스템 접근단계에서 종료단계까지의 일련의 과정에서 행한 모든 활동을 재생, 검토, 조사하는 제반 활동이다.
③ 공유 데이터베이스 계정 : 다수 사용자가 동일한 계정에 직접적으로 접속하는 것을 허용하는 계정이다.
④ 계정 잠김 시간 : 반복된 로그인 실패 시 재 로그인을 수행할 없도록 하는 시간이다.
⑤ 로그(log) : 시스템 사용에 관련된 전체의 기록, 즉 입출력 내용, 프로그램 사용 내용, 데이터 변경 내용, 시작시간, 종료시간 등의 기록이다.
⑥ 베이스라인(Baseline) : 시스템 또는 소프트웨어 등의 비정상적인 변경 등을 방지하기 위하여, 정상적으로 동작하는 상태의 시스템 또는 소프트웨의 백업이다.

⑦ 인증(authentication) : 제시된 사용자 고유번호(ID)의 유효성을 확인하여 사용 가능한 권한을 부여하는 절차이다.

⑧ 시스템 관리자 (System Administrator) : 시스템 운영체제 및 응용 어플리케이션 등을 관리하는 관리자 이다.

⑨ 정보보안 책임자 (Information Security Administrator) : 데이터베이스 보안 관련 정책을 설정하고, 데이터베이스 감사 자료에 관한 접근 통제 권한을 가진 정보보호 전담부서의 정보보안 책임자 이다.

⑩ Batch job : 프로그램을 올려놓고(load) 작업을 수행할 때 작업의 중단 없이 계속해서 컴퓨터를 점유하여 처리하는 작업이다.

⑪ CC(Common Criteria) : 1999년 6월 8일 ISO 15408 표준으로 채택된 정보 보호 제품 평가 기준이다.

⑫ 데이터베이스 (Database Management System) : 데이터베이스를 구성하고 이를 응용하기 위하여 구성된 소프트웨어 시스템이다.

⑬ DBA(Database Administrator) : 데이터의 효율적인 저장 및 저장된 데이터의 보호 등의 데이터베이스 관리 업무를 담당하는 데이터베이스 관리자 이다.

⑭ DDL(Data Definition Language) : SQL의 구성 요소로서 레코드 설계, 필드 정의, 파일 위치 등을 정의하는 데이터 정의어다.

⑮ SQL(Structured Query Language) : 데이터베이스의 조작과 관리에 사용되는 데이터베이스 하부 언어이다.

제2장 데이터베이스 무결성

제4조 소프트웨어 무결성

① 데이터베이스 패치관리

1) 데이터베이스 의 정상적인 동작을 지원하기 위하여서는 데이터베이스 실행파일 및 데이터 파일의 무결성이 보장되어야 한다.
특히, 데이터베이스 제조업체가 제공하는 최신의 패치를 적용함으로써 시스템의 알려진 취약점을 제거할 수 있다.

2) DBA는 데이터베이스 패치 수준을 시스템 영향도를 고려하여 최신 상태로 유지 하여야 한다.

3) 정보보안 책임자 또는 DBA는 지원되지 않는 데이터베이스 소프트웨어를 제조업체의 지원이 만료되기 전에 업데이트하거나 제거하여야 한다.

4) 정보보안 책임자 또는 DBA는 제조업체의 보안 패치지원 만료일 이전에 데이터베이스를 업데이트하기 위한 계획을 세워야 한다.

5) 정보보안 책임자는 데이터베이스 버전이 제조업체로부터 제공되는 최신의 패치들이 적용되었는지 확인해야 한다.

② 데이터베이스 소프트웨어/오브젝트 변경관리

1) 정보보안 책임자는 비인가 변조행위의 감지를 위하여 데이터베이스 소프트웨어를 해당 업체 또는 기관의 DBA 및 정보보안 책임자가 사전 협의한 최소 주기(예: 주간 단위)로 모니터링 해야 한다.

2) DBA는 호스트 시스템의 디렉토리 및 파일에 대한 베이스라인 및 모니터링을 위한 데이터베이스 소프트웨어 디렉토리 리스트를 시스템 관리자 및 정보보안 책임자에게 제공해야 한다.

3) 정보보안 책임자는 데이터베이스 소프트웨어 수정이 각 사업체 또는 공공 기관의 데이터베이스 소프트웨어 구성 관리 방침과 절차를 준수하였는지 확인해야 한다.

4) 정보보안 책임자는 데이터베이스 어플리케이션이 DDL을 사용하지 못하도록 제한하여야 한다.

5) 시스템 관리자는 서드파티 데이터베이스 어플리케이션이 데이터베이스 소프트웨어 및 데이터 파일과 분리된 논리적 파티션에 설치되도록 해야 한다.

제4조 소프트웨어 무결성

③ 사용하지 않는 데이터베이스 소프트웨어/컴포넌트

1) DBA는 사용하지 않는 데이터베이스 컴포넌트나 데이터베이스 소프트웨어를 데이터베이스 및 호스트 시스템에서 삭제하여야 한다.

제5조 데이터베이스 소프트웨어 개발

① DBA는 기존 시스템에서의 소프트웨어 개발 시 유일하게 인식되는 데이터와 어플리케이션 파일 저장 파티션과 프로세스/서비스에 대한 분리 사용을 준수해야 한다.

② 정보보안 책임자는 소프트웨어 구성 관리 방침에 의해 검증되지 않은 소프트웨어가 기존 시스템에 로딩되는 것을 규제해야 한다.

③ DBA는 기존 데이터베이스와 개발 데이터베이스 간의 데이터베이스 링크를 허가하지 않아야 한다.

④ DBA는 정보보안 책임자에게 보고되는 않은 개발 어플리케이션이 기존 데이터베이스에 접근하는 것을 방지해야 한다.

⑤ DBA는 기존 데이터베이스로부터 생성되는 데이터베이스의 패스워드를 변경해야 한다.

⑥ DBA는 기존 데이터베이스로부터 내보내기(export)된 데이터를 개발 데이터베이스에서 사용할 경우 급여 데이터나 개인정보와 같은 모든 민감한 데이터를 제거하거나 변경하여야 한다.

⑦ 정보보안 책임자는 어플리케이션 코드의 변경을 위하여 공유되는 기존/개발 데이터베이스 시스템에서 주어진 검토 권한의 적합성을 해당 업체 또는 기관의 DBA 및 정보보안 책임자가 사전 협의한 주기(예: 최소 3달 주기)로 검토하여 적용해야 한다.

⑧ DBA는 어플리케이션 개발자에게 기존 데이터베이스의 시스템 권한(데이터베이스의 생성, 변경 및 삭제 등의 권한)을 인가하여서는 안 된다. 단, 부득이하게 부여하여야하는 경우 소속팀장 및 정보보호 최고 책임자의 결재를 득한다.

제6조 비정형 질의

① 비정형 질의는 사용자가 데이터베이스에 시험되지 않는 명령을 실행할 수 있는 가능성을 제공할 수 있다. 이런 제한되지 않은 접근은 알려지지 않은 취약점에 데이터베이스가 노출될 수 있는 소지를 제공한다. 비정형 질의는 개발이 완료된 시스템에서는 허용되어서는 안 되며, 정형화된 프로시저를 통한 질의의 사용이 권고된다. 그러나, 데이터 웨어하우스와 같은 몇몇 데이터베이스 유형에서 비정형 질의가 요구될 수도 있다.

② 정보보안 책임자는 권한이 있는 DBA만이 비정형 질의를 할 수 있도록 관리하여야 한다.

제7조 다중 서비스 호스트 시스템

① DBA는 특정 서비스를 위한 지정된 서버에 데이터베이스를 설치하여야 한다.

② DBA는 가능하면 웹서버 또는 DNS서버와 같은 범용 서버 장비에 데이터베이스를 설치하지 않아야 한다.

제8조 데이터 무결성

① 데이터베이스 파일 무결성

1) 시스템 관리자는 제조업체가 권장하는 권한을 따라서 데이터베이스 소프트웨어 권한을 설정해야 한다.

2) 시스템 관리자는 데이터베이스의 설치에 의해 생성된 모든 디렉토리 및 파일에 대한 권한은 제조업체가 권장하는 지침에 의거하여 설정해야 한다.

3) 시스템 관리자는 데이터베이스 소프트웨어와 관련된 디렉토리 이름, 파일 권한 또는 그룹 정보의 변경 권한을 DBA로 제한하여야 한다.

② 데이터베이스 소프트웨어 베이스라인

1) 시스템 관리자 및 DBA는 데이터베이스 소프트웨어가 업데이트되었을 경우 데이터베이스 소프트웨어를 백업해야 한다.

③ 데이터베이스 파일 백업 및 복구

1) DBA는 모든 데이터베이스의 검증된 백업 전략을 구현해야 한다.

2) DBA는 데이터베이스 백업 및 복구 절차를 문서화해야 한다.

제3장 데이터베이스 암호화

제9조 데이터 암호화

① 데이터베이스에 포함된 데이터는 ‘해독 불가능’ 상태로 처리하여 부적절한 접근을 통한 데이터 유출에 대비한다.

② 데이터는 저장 장소에 관계없이 읽을 수 없도록 키 관리 프로세스 및 절차에 따른 강력한 암호 기법(예를 들면, 대칭키 암호 알고리즘, 일방향 해시(One-way hash))등의 방법을 통하여 처리되어야 한다.

③ 일반적으로 데이터베이스 암호화를 수행하면 데이터베이스의 검색 및 변경 등에서 성능 저하가 발생한다. 이를 최소화하기 위하여 컬럼 단위의 데이터베이스 암호화를 권장하나, 불가능할 경우 차선책으로 파일단위 암호화를 실행한다. 암호화에 적용되는 알고리즘은 암·복호화 속도가 빠른 대칭키 암호 알고리즘을 권장한다. 컬럼 단위 암호화는 성능 저하를 최소화하기 위하여 주요 데이터에 대하여 선택적으로 적용한다. 디스크 암호화가 사용되고 있다면 논리적인 접근은 운영체제 고유의 접근통제 메커니즘과 독립적으로 관리되어야 한다. 특히, 복호화 키는 사용자 계정과 관련되어서는 안 된다.

④ DBA는 민감한 데이터에 대하여 컬럼 단위의 암호화를 수행해야 한다. 부득이한 경우 파일 단위의 암호화 또는 데이터베이스에서 지원하는 기능인 TDE 를 이용하여 암호화를 수행할 수 있다.

제10조 백업 데이터 보호

① DBA는 전체 또는 부분 암호화하여 백업된 데이터 복구 시 복호화 방안에 대해 검토해야 한다. 백업 데이터의 저장 시 컬럼 단위 혹은 파일 단위의 암호화를 권장한다.

② 정보보안 책임자는 암호화된 백업 데이터의 접근 및 관리 권한이 시스템 운영 관리자에게만 제한됨을 주기적으로 확인하여야 한다.

③ 정보보안 책임자는 중요 백업 데이터 보안의 품질을 유지하기 위해 백업 데이터의 보안 등급을 일정 기간 단위로 강등하여 순차적으로 보안 해제할 수 있다.

④ DBA는 업무상 또는 법적으로 더 이상 필요 없을 경우 백업 데이터는 복원이 불가능한 방법으로 영구 폐기한다.

제11조 암호화 키 관리

① ~~DBA는~~ 암호키 접근 권한은 DBA, 엄호키관리자, 정보보안 책임자로 제한하며, 필요시 정보보안 책임자가 지정할 수 있다.

② DBA는 최소한의 접근만이 허용될 수 있는 장소에 안전하게 암호키를 보관해야 한다.

③ DBA는 아래 사항을 포함하여 데이터베이스 암호화에 사용되는 모든 키 관리 프로세스 및 절차를 문서화하며 이를 준수해야 한다.

1) 안전한 키 생성/ 분배/ 저장
2) 구버전 키 및 무효키 폐기
3) 이미 알려졌거나 알려졌을 것이라고 의심이 가는 키 교체
4) 비인가된 키 대체 방지
5) 키 보관자로 하여금 그들의 의무를 이해하고 관련 규정의 준수를 명시하는 문서를 마련하여 서명하도록 요청

제4장 데이터베이스 접근제어

제12조 데이터베이스 계정관리

① DBA는 모든 데이터베이스 활동 내역이 추적될 수 있도록 유지하여야 한다.

② DBA는 모든 데이터베이스 계정이 각각의 업무를 위한 최소한의 권한으로 유지되도록 하여야 한다.

③ DBA는 모든 데이터베이스 계정이 암호, 또는 다른 유효한 입증 방법에 의해 보호되도록 구성해야 한다.

④ DBA는 공유 데이터베이스 계정의 사용에 대하여 정보보안 책임자에게 승인 받아야 하며, 문서화하여야 한다.

제13조 인증

① 모든 데이터베이스 접속시 안전한 인증방식을 통해 접근한다.

② 일정 시간동안 입력이 없는 세션은「생활보안지침」제11조(사용자 인증 및 식별)에 따라 연결을 차단하여야 한다. 단, 예외가 있는 경우는 타당성을 검토하고 정보보안 책임자의 승인을 득하여 적용한다.

③ 모든 데이터베이스 접근권한은「생활보안지침」제9조(사용자 계정 및 접근권한 관리)에 따라 접근권한을 분류하여 업무 별 권한의 차등부여가 가능하여야 하며, 업무 목적에 맞게 접근권한 부여를 최소화하여야 한다.

제14조 패스워드 정책

① DBA는 데이터베이스 계정 생성시 임시 데이터베이스 계정 패스워드를 할당해야 한다.

② DBA는 데이터베이스 계정 패스워드가 암호 정책에 맞는지 확인해야 하며, 각 사용자가 임시 패스워드를 받을 때 암호 정책을 주지시켜야 한다.

③ DBA는 데이터베이스 계정 패스워드를 암호화하여 저장하여야 한다.

④ DBA는 데이터베이스 계정명과 데이터베이스 계정 패스워드가 호스트 커맨드 라인에서 평문으로 보이지 않도록 해야 한다.

⑤ DBA는 데이터베이스 계정 로그인은 해당 업체 또는 기관의 DBA 및 정보보안 책임자가 사전 협의한 횟수 (예: 3회) 실패 시 더 이상의 로그인을 수행할 수 없도록 설정하여야 한다.

⑥ DBA는 데이터베이스 계정 잠김 시간(반복된 로그인 실패 시 재 로그인을 수행할 없도록 하는 시간)을 정보보안 책임자에 의해 정의된 최소 잠김 시간 이상으로 설정한다

⑦ DBA는 데이터베이스 계정 패스워드의 길이가 해당 업체 또는 기관의 DBA 및 정보보안 책임자가 사전 협의한 길이 (예: 최소 8자) 이상의 숫자, 문자로 구성해야 하며, 대문자, 소문자, 숫자 및 특수문자를 포함하도록 설정해야 한다.

⑧ DBA는 데이터베이스 계정 패스워드는 이름, 전화번호, 계정명 등의 개인정보를 포함하지 않도록 설정해야 한다.

⑨ DBA는 데이터베이스 계정 암호가 연속적으로 반복되는 문자를 포함하지 않도록 설정하여야 한다.

⑩ DBA는 패스워드 변경 시 새로운 데이터베이스 계정 암호는 해당 업체 또는 기관의 DBA 및 정보보안 책임자가 사전 협의한 개수 (예: 최소 4개)의 문자가 이전 암호와 다른 것으로 설정하여야 한다.

⑪ DBA는 데이터베이스 계정 암호가 해당 업체 또는 기관의 DBA 및 정보보안 책임자와 사전 협의한 주기(예: 90일) 또는 더 빈번하게 교체되도록 설정하여야 한다.

⑫ DBA는 데이터베이스 계정 암호 교체 시 해당 업체 또는 기관의 DBA 및 정보보안 책임자와 사전 협의한 횟수(예: 10차례) 이내에서는 기존의 암호가 재사용하지 않도록 설정해야 한다.

⑬ DBA는 가능하다면 데이터베이스 계정 암호가 해당 업체 또는 기관의 DBA 및 정보보안 책임자와 사전 협의한 주기 (예: 1년) 또는 그 이상의 주기 미만으로 재사용되지 않도록 설정해야 한다.

⑭ DBA는 어플리케이션 데이터베이스 계정 암호가 적어도 일년에 한 번 또는 시스템 관리자가 변경되었을 경우 변경하여야 한다.

⑮ DBA는 데이터베이스 설치 시 생성된 모든 기본 데이터베이스 계정 암호를 변경해야 한다.

제15조 데이터베이스 계정

① DBA 계정

1) DBA는 모든 기본 설치 암호가 DBA 데이터베이스 계정에 남아 있지 않게 하여야 한다.
2) 정보보안 책임자는 DBA가 DBA 업무 만을 수행하기 위해 할당된 데이터베이스 계정을 사용하는지 확인해야 한다.
3) 데이터베이스 접속 시는 공용 ID를 사용하지 않고, 작업 수행자가 명료히 식별되도록 개인 ID로 접속해야 한다.

② 어플리케이션 오브젝트 소유/스키마 계정

1) DBA는 어플리케이션 사용자 데이터베이스 계정이 데이터베이스 오브젝트를 소유하지 않도록 해야 한다.
2) DBA는 특정 어플리케이션 오브젝트 소유자 계정은 어플리케이션 오브젝트의 업데이트나 유지보수에만 사용되도록 해야 한다.
3) DBA는 특정 어플리케이션 소유자 계정이 사용되지 않을 경우 해당 권한을 제거 혹은 비활성화하거나 계정을 잠금 처리하여야 한다.

제16조 데이터베이스 권한

① DBA는 어플리케이션 사용자에게 수여되는 모든 오브젝트 권한이 어플리케이션 특정 역할(role)의 사용으로 허용되는 것을 확인해야 한다.
② DBA는 오브젝트 권한을 개별적인 어플리케이션 사용자 데이터베이스 계정에 직접적으로 할당하지 않아야 한다.
③ DBA는 어플리케이션 오브젝트 권한이 PUBLIC으로 허용하지 않도록 설정해야 한다.
④ DBA는 데이터베이스 설치 디폴트 오브젝트 권한이 PUBLIC으로 허용되지 않도록 설정해야 한다.
⑤ 정보보안 책임자는 DBA계정의 DBA 뷰와 테이블에 대한 접근을 DBA로 제한하여야 한다.

제5장 데이터베이스 감사

제17조 데이터베이스 감사 일반사항

① DBA는 모든 데이터베이스 보안 관련 이벤트에 대한 데이터베이스 감사가 수행되고 있음을 확인해야 한다.

② 시스템 관리자 및 DBA는 데이터베이스 서비스 시작 및 종료 등과 관계된 데이터베이스 호스트 시스템의 감사가 수행되고 있음을 확인해야 한다

③ DBA는 감사 데이터를 정보보안 책임자가 인가한 인원만 열람할 수 있도록 해야 한다.

④ DBA가 수행하여야 할 최소한의 데이터베이스 감사 내용은 아래와 같다.

1) DBA는 데이터베이스 사용자 계정에 대한 생성, 변경 및 삭제에 대한 감사를 수행하여야 한다.

2) DBA는 데이터베이스 시스템 저장 구조, 테이블, 인덱스에 대한 생성, 변경 및 삭제에 대한 감사를 수행하여야 한다.

3) DBA는 데이터베이스 감사 기능 활성화 및 비활성화 기능에 대한 감사를 수행하여야 한다.

4) DBA는 데이터베이스 시스템 권한에 대한 인가 및 취소에 대한 감사를 수행하여야 한다.

5) DBA는 데이터베이스 오브젝트가 존재하지 않음으로 인하여 발생한 에러 이벤트에 대한 감사를 수행하여야 한다.

6) DBA는 데이터베이스 오브젝트의 이름을 변경하는 이벤트에 대한 감사를 수행하여야 한다.

7) DBA는 데이터베이스 계정으로부터 오브젝트 권한 인가 및 취소에 대한 감사를 수행하여야 한다.

8) DBA는 데이터베이스 데이터 디렉토리 변경에 대한 감사를 수행하여야 한다.

9) DBA는 데이터베이스 시스템 설정 변경에 대한 감사를 수행하여야 한다.

10) DBA는 모든 데이터베이스의 연결 실패에 대한 감사를 수행하여야 한다.

⑦ DBA 작업 감사

1) 정보보안 책임자는 데이터베이스 시작, 종료, 감사 데이터의 변경 및 삭제와 관련된 DBA의 활동에 대한 감사를 수행해야 한다.

2) 정보보안 책임자는 데이터베이스 온라인 백업과 관련된 DBA의 활동에 대한 감사를 수행해야 한다.

3) 정보보안 책임자는 데이터베이스 압축과 관련된 DBA의 활동에 대한 감사를 수행해야 한다.

4) 정보보안 책임자는 데이터베이스 성능 정보 수집과 관련된 DBA의 활동에 대한 감사를 수행해야 한다.

제18조 감사 데이터 백업

① DBA는 감사 데이터 삭제 작업의 원인에 대하여 감사 추적을 위한 감사 레코드를 작성해야 한다.

② DBA는 감사 데이터 삭제 기능이 현재의 감사 데이터를 삭제하지 않음을 확인해야 한다

제19조 감사 데이터 검토

① DBA 또는 시스템 관리자는 현재의 감사 데이터를 제공하여야 한다.

② DBA 또는 시스템 관리자는 감사 데이터 히스토리를 제공하여야 한다.

③ DBA 또는 시스템 관리자는 현재의 감사 데이터를 백업하는 절차 및 방법을 제공하여야 한다.

제20조 감사 데이터 접근

① DBA는 감사 정보를 볼 수 있는 DBA 뷰의 권한을 DBA나 정보보안 책임자로 제한하여야 한다.

② DBA는 감사 정보에 대한 조회 및 변경 권한(예: 선택, 삽입, 삭제 및 갱신 등의 권한)을 DBA나 정보보안 책임자로 제한하여야 한다.

③ DBA는 감사 기능을 비활성화 시키는 권한을 DBA나 정보보안 책임자로 제한하여야 한다.

제21조 데이터베이스 모니터링

① 시스템 관리자나 DBA는 비인가된 batch job이나 스크립트가 데이터베이스에서 수행되지 않는 지 해당 업체 또는 기관의 DBA 및 정보보안 책임자가 사전 협의한 기간(예: 매일) 단위로 프로세스 리스트를 점검하여야 한다.

② DBA는 batch job과 스크립트가 암호화되지 않은 포맷의 패스워드를 저장하는지 감시해야 한다.

③ DBA는 비인가 어플리케이션에 의한 접근 및 데이터베이스 오브젝트의 비인가 수정을 모니터링 해야 한다.

④ DBA는 만료된 데이터베이스 계정과 사용하지 않는 데이터베이스 계정을 모니터링 하고 사용하지 않는 계정은 계정 정책에 의거하여 제거해야 한다.

제6장 데이터베이스 운영 환경

제22조 네트워크 접속 환경

① 네트워크를 통한 데이터베이스 접속

1) 정보보안 책임자는 네트워크를 통한 데이터베이스 접속이 수행되는 경우, 클라이언트가 제공하는 계정 이름과 데이터베이스 접근을 위한 인증 데이터(예: 패스워드)가 암호화 되는 지 확인해야 한다.

2) 정보보안 책임자는 사용자의 네트워크를 통한 데이터베이스 접속이 수행될 때, 인증 절차를 거치는 지 확인해야 한다.

3) DBA는 데이터베이스의 원격 관리자 접속 연결을 암호화하여야 한다.

② Open Database Connectivity(ODBC)

1) ODBC는 어떤 응용 프로그램을 사용하는지에 관계없이, 데이터베이스를 자유롭게 사용하기 위하여 만든 응용 프로그램의 표준방법으로서 데이터베이스를 접근하는 또 다른 방법이다.

2) DBA는 사용하지 않는 ODBC 실행 파일을 데이터베이스 서버에서 삭제하여야 한다.

3) 정보보안 책임자는 ODBC의 접속 시 비암호화된 패스워드는 저장되지 않음을 확인해야 한다.

③ 네트워크 접속 세션 시간 관리

1) DBA는 데이터베이스 네트워크 접속 세션 타임 아웃 시간을 해당 데이터베이스를 사용하는 평균 시간 이내로 지정하여야 한다.

2) DBA는 데이터베이스 네트워크 접속 세션 타임 아웃 시간을 비활성화하는 행위를 감시하여야 한다.

제23조 운영체제

① 시스템 관리자는 데이터베이스 실행 파일, 데이터베이스 설정 파일 및 데이터베이스 데이터 파일에 대한 접근을 데이터베이스 제공업체의 보안 요구 사항을 만족하도록 설정하여야 한다.

② 시스템 관리자는 운영체제 어플리케이션 레벨 계정을 데이터베이스 어플리케이션 파일만 접근이 가능하도록 해야 한다.

③ 시스템 관리자는 운영체제 관리자 레벨 계정을 데이터베이스 제공업체의 보안 요구 사항을 준수하여 설정하여야 한다.

④ 정보보안 책임자는 인가된 DBA만이 데이터베이스 관리 권한 운영체제 그룹에 속해 있음을 확인해야 한다.

⑤ 정보보안 책임자는 데이터베이스 소프트웨어 설치 계정에 대한 접근은 인가된 DBA만이 가능하도록 해야 한다.

⑥ 정보보안 책임자는 데이터베이스 소프트웨어 설치 계정의 작업 내용의 로그가 저장되도록 설정해야 한다.

제7장 데이터베이스 사고 대응

제24조 데이터베이스 사고시 보고

① DBA는 업무 수행 시 발생되는 데이터베이스 보안 관련된 모든 문제점과 위반 사항에 대하여 데이터베이스 사용자 및 정보보안 책임자에게 즉시 보고하도록 사고 대응 절차를 수립해야 한다.

제25조 사고대응

① 정보보안 책임자는 데이터베이스에 접근되는 모든 네트워크 접속을 차단해야 한다.
② DBA는 감사 데이터 검토 등을 통하여 보유 전산 데이터 및 전산장비에 대한 변조, 파손, 불법 유출 등에 대한 조사를 수행해야 한다.
③ DBA는 데이터베이스 시스템의 바이러스등의 악성 코드 감염여부를 조사해야 한다.
④ DBA는 백업 데이터를 이용하여 데이터베이스 복구작업을 수행해야 한다.
⑤ DBA는 데이터베이스를 관리하는 주요 권한을 가진 계정(예: DBA)의 패스워드를 변경해야 한다.