로그 관련 업무 지침

개정이력

|  |  |  |  |
| --- | --- | --- | --- |
| No. | 개정 사유 및 내용 | 개정일자 | 담당자 |
| 1 | 제정 | 2024.04.05 | 최철훈 |
|  |  |  |  |

목차

[목적 3](#_Toc13595542)

[범위 3](#_Toc13595543)

[제1조 (시간 동기화) 3](#_Toc13595544)

[제2조 (정보시스템 로그기준 정의) 3](#_Toc13595545)

[제3조 (보관 및 백업) 4](#_Toc13595546)

[제4조 (로그검토) 4](#_Toc13595547)

# 목적

본 지침은 주식회사 제타큐브(이하 '회사') 소유의 정보시스템 로그 및 데이터의 검토/백업 등에 대한 통제를 구성하고 관리하는 방법들을 정함으로써 회사의 사업 연속성을 보장하고 사업 손실을 최소화하는데 있다.

# 범위

회사의 사업장 내의 모든 정보시스템을 그 적용범위로 하며, 적용범위 내의 모든 자원을 이용하여 정보전달을 행하는 모든 사용자 및 정보시스템을 그 대상으로 한다.

# 제1조 (시간 동기화)

1. 정보시스템의 시각을 내부 또는 외부의 NTP서버와 동기화하여야 한다.

# 제2조 (정보시스템 로그기준 정의)

1. 정보시스템에서 발생되는 로그에 대한 관리는 다음을 따른다.

가. 로그유형: 계정 관련, 권한관련, 접근, 액션, 시스템, 구매/취소이력

나. 보존기간: 12개월 이상을 원칙으로 한다. 단, 구매 관련한 로그는 5년간 보관을 해야 한다.

다. 보존방법: 도난, 분실되지 않도록 안전하게 보관한다.

2.(법) 다음 로그 유형은 각 로그 보존기간을 적용하여야 한다.

가. 개인정보처리시스템에 대한 사용자 계정 및 권한에 대한 추가, 수정, 삭제 내역: 3년 이상

나. 개인정보 취급자가 개인정보처리시스템에 접속한계정, 접속일시, 접속지정보, 처리한 정보주체정보, 수행업무의 접속기록: 12개월 이상

다. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 접속기록: 24개월 이상

라. 5만명 이상의 고객의 개인정보를 처리할 경우에 모든 개인정보처리시스템의 접속기록: 24개월 이상

# 제3조 (보관 및 백업)

1. 정보시스템의 가용성 및 데이터의 무결성을 유지하기 위해 다음과 같은 백업절차를 따른다.

가. 백업대상: 접속기록, DB데이타, 설정파일, 파일시스템

나. 주기: 6개월 단위를 기본으로 한다. 단, 자동화 백업이 가능할 경우에는 일일백업 또는 주일백업 등을 실시한다. 또한, 중요한 변화가 발생된 이후에는 백업을 진행한다.

다. 방법: 최초 1회 풀 백업을 진행 후 차등백업을 기본으로 하며, 개인정보 등 중요 데이터에 대해서는 소산백업을 진행한다. 특히, 월랫운영과 관련된 데이터도 소산백업을 진행한다.

라. 보존기간: 최소 6개월을 기본으로 한다. 단, CCTV 데이터에 대해서는 예외로 할 수 있다.

2. (법) 개인정보처리시스템의 로그(접속기록 등)는 백업 시 위변조 여부를 확인할 수 있는 방식(Read-Only 매체사용, 해쉬값 적용, 백업매체 접근제어, 위변조 방지 솔루션 등)을 적용하여야 한다.

3. 정보시스템에서 발생되는 모든 로그는 별도의 시스템 또는 매체에 백업하여 보존기간 이상만큼 보관하여야 한다.

4. 정보시스템 계정, 정보시스템의 사용자계정 및 중요정보에 대한 접근권한 부여 및 변경(퇴직 및 휴직, 직무변경, 부서변경 등)에 대한 이력을 남겨야 한다.

5. 백업된 정보시스템의 데이터가 정상적으로 복구될 수 있도록 복구 테스트를 진행한다.

# 제4조 (로그검토)

1. 정보시스템에 대한 사용자 로그 검토 기준은 다음과 같다.

가. 접근의 타당서(업무시간 외 접속 등)

나. 불법적인 유출시도(미승인 계정의 접속시도 등)

다. 오남용(개인정보 과다 조회 등)

2. 정보시스템에 대한 사용자 접근이 업무상 허용된 범위에 있는지를 다음을 따라 확인한다.

가. 모니터링 대상: 접속기록, 액션로그

나. 모니터링 방법: 사용자 로그 검토 기준적용

다. 모니터링 주기: 반기 1회 이상 진행. 단, 개인정보처리시스템인 경우에는 월1회 이상 진행[시행일자: 24년 9월 15일]. 특히, 월렛과 관련된 정보처리시스템인 경우에도 월1회 이상 진행.

라. 모니터링 보고: 해당 자산 관리자가 검토하여 그 결과를 (개인)정보보호관리자에게 보고. 특히, 개인정보 다운로드 점검기준에 해당하는 다운로드가 발견된 경우에는 사유를 확하여 보고해야 함[시행일자: 24년 9월 15일]. (개인정보 다운로드 점검기준: 통상적인 개인정보 일평균건수보다 3배 이상의 개인정보를 다운로드 한 경우, 1시간 이내 일평균건수의 50%에 해당하는 개인정보를 다운로드 한 경우, 새벽시간/휴무일 등 업무시간 외 개인정보를 다운로드 한 경우)

3. 정보시스템 계정, 정보시스템의 사용자계정 및 중요정보에 대한 접근권한 부여가 적정하게 이루어 졌는지를 반기별로 자산 관리자가 점검한 후 자산 책임자에게 보고한다.

4. 정보시스템 계정, 정보시스템의 사용자계정 및 중요정보에 대한 접근권한 변경(퇴직 및 휴직, 직무변경, 부서변경 등)이 적시에 이루어 졌는지를 반기별로 자산 관리자가 점검한 후 자산 책임자에게 보고한다.

5. 정보시스템 계정, 정보시스템의 사용자계정 및 중요정보에 대한 계정이 3개월간 미 사용된 경우에는 이에 대한 적정성 여부를 자산 관리자가 확인한 후 자산 책임자에게 보고한다. 단, 시스템에 의해 자동 적용된 경우에는 별도보고를 하지 않아도 된다.

6. 정보시스템 로그검토 결과 이상징후가 포착될 경우 해당 관련자의 해명요구를 진행한다.

7. 해당 관련자의 해명요구와 이상징후 상황을 종합한 결과를 책임자에게 보고한다.