개발 관련 업무지침

개정이력

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

목차

[목적 3](#_Toc13596016)

[범위 3](#_Toc13596017)

[제1조 (개발 시 보안요구사항) 3](#_Toc13596018)

[제2조 (소스프로그램 접근관리) 5](#_Toc13596019)

[제3조 (시험데이터) 5](#_Toc13596020)

[제4조 (보안 요구사항 검토) 6](#_Toc13596021)

[제5조 (응용프로그램 이관) 6](#_Toc13596022)

# 목적

본 지침은 주식회사 제타큐브(이하 '회사')의 응용프로그램 개발 시 검토되어야 할 개발요구사항을 소프트웨어 수명주기에 따라 프로그램의 보안성, 안정성, 신뢰성을 확보하는데 그 목적이 있다.

# 범위

본 지침은 회사에서 사용되기 위해 개발되는 모든 응용프로그램을 그 적용대상으로 한다.

# 제1조 (개발 시 보안요구사항)

1. 어플리케이션 개발 시 설계 단계에서부터 다음과 같은 보안요구사항들이 고려되어야 한다.

가. 사용자/이용자 계정생성 관련된 보안요구사항(ID 생성규칙 기능, 패스워드 강도 설정 기능, 패스워드 변경 주기 기능, 장기 미사용자 계정 락 기능, 세션 타임아웃 설정 기능, 로그인 연속실패시 락 설정 기능 등)

나. 접근권한 최소화 설정 관련된 보안요구사항(접근권한을 그룹/인원/메뉴 별 세부적으로 부여하여 인원 별 읽기/수정/삭제/다운로드를 세부적으로 구분하여 적용할 수 있도록 지원하는 기능)

다. 감사증적 확보와 관련된 보안요구사항(계정에 대한 생성/삭제에 관한 로그, 계정에 대한 권한의 등록/변경/삭제에 관한 로그, 계정의 로그인/액션/로그아웃에 관한 로그 등)

라. 개인정보를 외부망을 통해 전송 시 암호화(HTTPS 또는 암호모듈 등)하여 전송

마. 암호화 저장 대상항목에 대해 안전한 양방향 암호 알고리즘(SEED, ARIA 등)을 사용

바. 패스워드를 저장 시 SHA256 등 안전한 일방향 암호 알고리즘으로 암호화

사. 회원의 개인정보를 다량으로 조회/출력 시 마스킹이 적용(성명: 홍\*동, 생년월일: \*\*\*\*년 \*월 \*일, 전화번호: 02-\*\*\*\*-1234, 핸드폰: 010-\*\*\*\*-1234, 주소: 서울 종로구 \*\*\*동 12-3, 접속지IP: 123.123.\*\*\*.123)

아. DB와의 연동을 위해 DB계정/패스워드를 프로그램 코딩 상에 포함(하드코딩)시키지 않도록 함

자. 개발에 사용되는 코딩방법으로 시큐어코딩이 적용

2. 개인정보 수집 시 다음과 같은 정상적인 개인정보 양식만이 입력 받을 수 있도록 시스템이 구성되어져 있어야 한다.

가. 생년월일 입력에 현시점보다 더 늦은 년도가 입력되지 않도록 함

나. 입력란에 특수문자 또는 010이 아닌 구분자가 들어가지 않도록 함

다. 이메일 입력란에 특수문자 또는 123@@gmail.com 같이 이메일 양식에 맞지 않는 입력 값이 들어가지 않도록 함 등

3. 정보주체가 본인의 개인정보를 최신정보로 수정할 수 있도록 시스템이 구성되어져 있어야 한다.

4. (법) 개인정보를 조회 또는 출력(인쇄, 화면표시, 파일생성 등)할 수 있는 개인정보처리시스템일 경우, 개인정보취급자(사용자)가 개인정보의 조회, 출력 등의 업무를 다량으로(정보주체 세부현황 조회 시 제외) 수행할 때 다음의 내용을 적용하여 개인정보를 마스킹하여 표시제한 조치를 취할 수 있도록 구성되어져 있어야 한다.

가. 성명 중 이름의 첫 번째 글자 이상(홍\*동)

나. 생년월일(\*\*\*\*년 \*\*월 \*\*일)

다. 전화번호 또는 휴대폰 전화번호의 국번(02-\*\*\*\*-1234, 010-\*\*\*\*-1234)

라. 주소의 읍.면․동(서울시 강남구 \*\*동 60번지)

마. 인터넷주소는 버전 4의 경우 17～24비트 영역/버전 6의 경우 113～128비트 영역(123.123.\*\*\*.123) 등

5. 개인정보를 조회 또는 출력할 수 있는 개인정보처리시스템일 경우, 개인정보를 조회/출력 시 불필요한 과도한 정보주최(이용자)의 정보가 조회되지 않도록 일치검색 또는 두가지 항목 이상의 검색조건을 통해서만 진행될 수 있도록 구성되어져 있어야 한다.

6. (법) 개인정보를 조회 또는 출력(인쇄, 화면표시, 파일생성 등)할 수 있는 개인정보처리시스템일 경우, 정보주체의 개인정보를 조회 시 해당 정보주체의 모든 개인정보가 조회 또는 출력되지 않고 꼭 필요한 용도에 해당하는 개인정보 항목만이 조회 또는 출력되도록 구성되어져 있어야 한다.

7. 어플리케이션 업그레이드 등 변경 시 보안요구사항은 어플리케이션 개발 시 보안요구사항을 준용하여 진행하여야 한다.

# 제2조 (소스프로그램 접근관리)

1. 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 접근권한을 설정하여야 한다.

# 제3조 (시험데이터)

1. 시스템 시험 과정에서 사용되는 시험데이터에는 실 운영데이터가 존재해서는 안된다.

2. 실제 운영 데이터를 시험 환경에서 사용하고자 할 경우에는 다음과 같은 절차에 따라 진행한다.

가. 정보보호 책임자로부터 사용 승인 진행

나. 시험을 위한 담당자만이 시험데이터에 접근 가능하도록 접근통제 설정

3. 실 운영DB를 테스트 DB로 사용하고자 할 경우, 업무에 필요한 최소한의 개인정보 항목에 국한하여 사용되어야 한다.

4. 테스트DB상에 테스트와 상관없는 개인정보 항목에 대해서는 비 식별화처리가 되어져 있어야 한다.

5. 실제 운영 데이터를 시험 환경에서 사용하고자 할 경우 실 운영 데이터베이스에 적용되는 보호대책과 동일한 수준으로 테스트 데이터베이스에도 해당 보호대책(접근통제 최소화, 암호화, 로깅 등)이 적용되어야 한다.

6. 실제 운영 데이터를 시험 환경에서 사용한 경우, 시험 완료 후 시험용 운영 데이터를 즉시 폐기하고, 폐기하였음을 실제 운영 데이터베이스의 자산책임자에게 보고하여야 한다.

# 제4조 (보안 요구사항 검토)

1. 어플리케이션 개발 완료 후 분석 및 설계 과정에서 도출한 보안요구사항이 모두 적용되었는지 확인하여야 한다.

2. 어플리케이션 개발 완료 후 보안요구사항에 대한 적용유무 확인 시 발견된 문제점에 대한 개선조치를 수행하여야 한다.

3. 메이저급 이상의 어플리케이션 변경개발 및 신규 어플리케이션 개발시 취약점 점검을 실시하고 도출된 취약한 상황에 대해 대응완료 후 운영환경으로 이관을 하여야 한다. 만약, 취약점 점검결과 취약한 상황을 대응하지 않고 운영환경으로 이관을 하고자 할 경우에는 책임자의 승인을 득해야 한다.

# 제5조 (응용프로그램 이관)

1. 시험을 통해 개발 또는 변경이 완료된 응용프로그램을 운영환경으로 이관시에는 다음의 절차에 따라 진행한다.

가. 개발자 이외의 별도의 이관담당자 선정

나. 이관이 원활하게 이루어지지 않았을 경우 복귀(rollback)를 위한 기존 운영시스템에 대한 백업진행

다. 이관이 성공적으로 이루어 진 이후에는 이관에 대한 책임자에게 보고함. 단, 마이너급의 단순이관일 경우에는 보고없이 이루어 질 수 있음

2. 신규 개발 또는 변경 시 운영환경에서 실행될 실행코드는 시험과 사용자 인수가 모두 완료된 이후에 실행되어야 한다.

3. 운영환경에는 승인되지 않은 개발도구(컴파일러, 편집기 등)와 소스코드(백업본 포함)가 있어서는 안되며 승인된 실행파일만 설치하여야 한다.