운영 관련 업무 지침

개정이력

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

목차

[목적 3](#_Toc151546150)

[범위 3](#_Toc151546151)

[제1조 (정보시스템 반/출입) 3](#_Toc151546152)

[제2조 (최신패치) 4](#_Toc151546153)

[제3조 (변경관리) 5](#_Toc151546154)

[제4조 (암호화) 5](#_Toc151546155)

[제5조 (공개서버의 정보공개) 6](#_Toc151546156)

[제6조 (전자거래/핀테크 제공) 7](#_Toc151546157)

[제7조 (가명정보/익명정보 처리) 7](#_Toc151546158)

[제8조 (보안시스템 운영) 8](#_Toc151546159)

[제9조 (보조저장매체 사용) 8](#_Toc151546160)

[제10조 (정보자산의 재사용) 9](#_Toc151546161)

[제11조 (취약점 점검) 9](#_Toc151546162)

# 목적

본 지침은 주식회사 제타큐브(이하 '회사') 소유의 정보시스템 운영에 대한 책임과 권한 및 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 (정보시스템 반/출입)

1. 신규 정보시스템(서버, 네트워크 장비, 어플리케이션 패키지, 정보보호시스템 등) 도입 시 다음과 같은 보안요구사항을 선별하여 인수기준을 수립한다.

가. 접근통제 설정 기능: 제품 디폴트 계정 제거, 관리자 접속 시 아이디/패스워드 인증, IP 기반 접속 통제, 세션 자동아웃 시간 설정

나. 패스워드 설정 기능: 패스워드 최소길이, 생성 방법, 변경주기 설정, 로그인 실패시 잠금 기능

다. 암호화 기능: 패스워드 일방향 암호화 저장, 접속 프로토콜의 구간 암호화, 중요 설정값의 암호화 저장

라. 사용자 로깅 기능: 계정 로그, 권한부여 로그, 접속로그, 액션로그, 시스템로그

마. 기타 정보시스템별 필요한 보안기능

2. 해당 정보시스템의 자산 관리자는 도입시 인수기준에 의한 적합성 여부를 검토한다.

3. 정보시스템 도입 시 기술적 취약점 진단을 실하여 위험도가 높은 모든 취약한 상황에 대해 대응을 완료한 이후 인수를 진행하여야 한다.

4. 정보시스템 도입 시 최신 패치를 적용 후 해당 정보시스템을 인수하여야 한다.

4의1. 정보시스템 도입 시 정의된 보안 요구사항(기술적 취약점 진단, 법적 요구사항 준수 등)에 적합한지를 검토하여야 한다.

4의2. 정보시스템 도입 시 정의된 보안 요구사항(기술적 취약점 진단, 법적 요구사항 준수 등)에 적합한지를 검토 후, 개선조치가 필요한 경우에는 개선조치를 수행 후 인수확인을 진행해야 한다.

5. 회사 자산에 정식 등록되지 않은 정보시스템을 통제구역/제한구역내 반입을 금한다. 단, 테스트 등을 위한 정보시스템을 반입하고자 할 경우에는 해당 부서장의 승인을 통해 반입할 수 있다.

6. 회사 자산에 등록된 정보시스템을 반출할 경우에는 유지보수/폐기 등 사유를 확인하고 자산책임자의 승인을 통해 반출하여야 한다.

7. 보호구역 내 정보시스템에 대한 반출입 현황을 출입관리대장에 남기고, 이를 정보보호 담당자가 월1회 검토한다.

# 제2조 (최신패치)

1. 정보시스템에 대한 최신 패치 발생 유무를 지속적으로 파악하여야 한다.

2. 서버에 설치된 소프트웨어, 운영체제, 정보보호시스템 등의 벤더사로부터 중요패치가 발생되는 경우에는 시스템에 미치는 영향을 사전분석 후 판단하여 실시한다. 단, 임대서비스를 받고 있는 서버에 한해서는 임대서비스 업체에 중요패치를 요청하여 진행한다.

3. 소프트웨어, 운영체제, 보안시스템 등에 대한 패치는 다음을 따른다.

가. PC에 설치된 소프트웨어, 정보보호시스템 등의 패치는 벤더사의 업데이트 방법을 따라 시행한다.

나. PC에 설치된 운영체제의 중요패치는 최신으로 업데이트 되도록 시행한다.

4. (법) 정보시스템에 대한 패치작업은 주기적으로 진행하여야 한다.

5. 정보시스템에 대한 패치작업 전 영향분석 등을 통하여 최신패치를 운영환경에 적용하기 어려울 경우에는 보완대책을 마련하여야 한다.

# 제3조 (변경관리)

1. 서버, 네트워크, 어플리케이션, 정보보호시스템(정책 업데이트, 룰셋변경 등) 등 정보시스템 관련한 변경절차는 다음을 따른다.

가. 정보시스템 자산 관리자가 변경계획을 수립하여 소속 부서장의 승인을 받는다. 단, 단순오류 수정 등에 대한 업무에 대해서는 선 처리 후 보고를 진행할 수 있다.

나. 롤백준비 후 변경작업을 진행한다.

다. 변경 작업 후 결과를 소속 부서장에게 보고한다.

2. 정보시스템의 큰 변경시에는 전반적인 성능 및 보안에 미치는 영향(기술적 취약점 점검 등)을 분석한다. 단, 정보시스템의 소규모 하드웨어 업그레이드(메모리, HDD추가 등), 단순수정 또는 PC에 대한 소프트웨어 패치 같은 업무는 제외한다.

# 제4조 (암호화)

1. 조직의 중요정보 보호를 위하여 다음과 같은 내용이 이행되어야 한다.

가. 암호화대상: 기밀문서, 개인정보가 포함된 문서

나. 암호강도(복잡도): KISA에서 제공한 '암호 알고리즘 및 키 길이 이용 안내서'를 준용한다.

2. (법) 다음과 같이 암호화 관련한 법적 요구사항을 개인정보의 저장 및 전송 시 반영하여야 한다.

가. 대상: 패스워드, 생체인식정보, 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호

나. 암호알고리즘: 패스워드(일방향 암호알고리즘), 그 외 대상(양방향 암호알고리즘)

3. (법) 모든 개인정보 및 인증정보(아이디, 패스워드 등)를 정보통신망을 통해 송수신시 암호화가 적용되어야 한다.

4. (법) 주민등록번호는 수집할 수 없으며 기존에 수집한 주민등록번호는 모두 삭제해야 한다. 만약, 특정 법률에 따라 주민등록번호를 수집해야만 할 경우에는 암호화하여 보관하여야 한다.

5. 고객의 개인정보가 포함된 파일을 PC등에 보관시에는 암호화 또는 패스워드 설정을 하여 보관하여야 한다.

6. 암호키에 대한 관리 절차는 다음을 따른다.

가. 생성: 암호키의 사용이 필요한 경우 정보보호책임자의 결재를 받아 암호키 생성 담당자에게 요청한다.

나. 이용: 암호키를 소스코드에 하드코딩해서는 안된다.

다. 보관

1) 암호키 생성 담당자는 암호키 생성 시 백업을 받아 시건장치가 있는 곳에 소산 백업한다.

2) 암호키의 사용기간은 5년으로 하며 정보보호위원회의 승인을 통해 사용기간을 연장할 수 있다.

라. 배포: 암호키 생성 담당자는 암호키를 생성하여 안전하게 요청자에게 전달한다.

마. 파기

1) 암호키가 분실/도난/유출되거나 암호시스템의 해킹이 의심되는 경우는 즉시 암호키를 변경하여야 한다.

2) 암호키의 사용기간이 끝나거나 암호키를 변경한 경우 암호키를 파기한다.

7. 암호키 복구가 필요한 경우 암호키 생성 담당자에게 공식적인 요청을 하며, 암호키 생성 담당자는 백업된 암호키로부터 복구를 진행한다.

# 제5조 (공개서버의 정보공개)

1. 웹사이트 등에 정보를 공개하는 경우 다음과 같은 절차를 따른다.

가. 기밀정보(개인정보 포함)

1) 수집: 기밀정보의 담당자(생성자)에게 정보의 수집을 요청한다.

2) 저장: 기밀정보는 암호화해서 저장하고 전달한다.

3) 공개: 기밀정보를 공개 시 정보보호담당자의 승인을 통해 진행된다. 단, 개인정보가 포함된 기밀정보일 경우에는 정보보호관리자의 승인을 통해 진행되며, 마스킹 룰을 적용해야 한다. (성명: 홍\*동, 생년월일: \*\*\*\*년 \*월 \*일, 전화번호: 02-\*\*\*\*-1234, 핸드폰: 010-\*\*\*\*-1234, 주소: 서울 강남구 \*\*\*동 12-3, 접속지IP: 123.123.\*\*\*.123)

나. 대외비정보

1) 수집: 대외비정보의 담당자(생성자)에게 정보 수집을 요청한다.

2) 저장: 대외비정보는 사내에서는 일반적으로 저장한다.

3) 공개: 대외비정보를 공개 시 정보 담당자(생성자)의 상위권자에게 고지 후 진행된다

# 제6조 (전자거래/핀테크 제공)

1. 전자거래 및 핀테크 서비스 제공 시 정보유출, 데이터 조작, 사기 등의 침해사고를 예방하기 위해 다음의 보호대책을 적용하여야 한다.

가. 암호화: 개인정보, 인증정보, 결제정보 송수신시 구간 암호화를 적용

나. 부인방지: 구매 및 취소 이력을 관리

2. 전자거래 및 핀테크 서비스 제공 시 결제시스템 등 외부 시스템과의 연계가 필요한 경우에는 외부 시스템(PG사 등)에서 제공한 모듈의 안전성으로 보호대책을 대체한다.

# 제7조 (가명정보/익명정보 처리)

1. 가명정보를 처리 시 특정 개인을 알아볼 수 없도록 처리하여야 한다.

2. (법) 가명정보 처리 시 원래의 상태로 복원하기 위한 추가정보는 가명정보와 분리보관(또는 삭제)하여야 한다.

3. (법) 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지 및 지체없이 회수/파기하여야 한다.

4. 가명정보 처리목적 등을 고려하여 가명정보의 처리 기간을 적정한 기간으로 정할 수 있다.

5. 개인정보를 익명처리 시 다른 정보를 사용하여도 더 이상 특정 개인을 알아볼 수 없도록 적정한 수준으로 처리하여야 한다.

# 제8조 (보안시스템 운영)

1. 최신 정책 업데이트, 룰셋변경 등 보안시스템의 운영절차는 다음을 따라 시행한다.

가. 보안시스템 자산 관리자가 적용계획을 수립하여 소속 부서장의 승인을 받는다.

나. 롤백준비 후 변경작업을 진행한다.

다. 변경 작업 후 결과를 소속 부서장에게 보고한다.

2. 보안시스템에 대한 정책적용 현황이 합당한지를 반기별로 점검해야 한다.

# 제9조 (보조저장매체 사용)

1. 휴대용 저장매체의 사용 절차는 다음을 따른다.

가. 휴대휴대용 저장매체를 연결하는 대상시스템: 개인정보 또는 지갑과 관련된 정보시스템 및 단말기에 대해서는 휴대용 저장매체 사용을 원칙적으로 금지한다. 단, 업무상 필요 시에는 예외신청을 통해 사용 가능하다.

나. 취급

1) 회사의 자산에 등록된 휴대용 저장매체만을 사용하도록 한다.

2) 대상시스템의 휴대용 저장매체를 연결할 수 있는 포트를 보안씰 등 물리적 또는 논리적으로 막는다.

3) 대상시스템의 CD라이터는 논리적 또는 물리적으로 제거한다. 단, 로그 백업용 등으로 사용하는 것은 예외로 한다.

4) 업무상 읽기/쓰기 등 필요한 경우에는 책임자의 사전승인을 통해 이용할 수 있다.

다. 보관: 휴대용 저장매체의 자산 관리자가 보관한다.

라. 폐기: 저장매체 폐기절차를 따르며 동일업무 범위 내에서는 재사용이 가능하다.

2. 휴대용 저장매체를 통한 악성코드 감염 방지에 대한 대책은 다음을 적용한다.

가. 휴대용 저장매체 자동실행 기능을 해지한다.

나. 이동식 저장매체 연결시 사용전에 백신검사를 수행한다.

3. (법) 휴대용 저장매체는 자산관리자가 보관하며, 보관 시 시건장치가 달려있는 안전한 위치에 보관하여야 한다.

4. (법) 보조저장매체를 자산관리자로부터 반출해서 사용하는 자도 시건장치가 달려있는 안전한 위치에 보관하여야 한다.

# 제10조 (정보자산의 재사용)

1. 하드디스크, 스토리지, 테잎 등 정보자산의 재사용 절차는 다음을 따른다.

가. 자산관리자가 자산책임자에게 정보자산의 재사용을 요청한다.

나. 자산관리자는 정보자산을 재사용하기 전에 로우포맷 등을 통해 중요정보를 삭제하여야 한다.

2. 하드디스크, 스토리지, 테잎 등 정보자산의 폐기 절차는 다음을 따른다.

가. 자산관리자가 자산책임자에게 저장매체 폐기를 요청한다.

나. 자산관리자는 자산관리 관련부서(총무부 등)에 저장매체의 물리적 폐기를 요청한다.

다. 자산관리 관련부서는 저장매체를 물리적으로 폐기 후 결과를 자산책임자에게 보고한다.

# 제11조 (취약점 점검)

1. 자산구분 중 Linux서버/Win서버/네트워크장비/DBMS/WEP에 해당하는 범위 내 자산에 대한 취약점 점검은 년1회 이상 정기적으로 진행하여야 한다. 그리고, 그 외 자산구분에 해당하는 범위 내 자산에 대해서는 인증기준 및 법률 요구사항에 근거한 기본통제 접근법(Baseline Approach)을 적용하는 것으로 취약점 점검을 갈음할 수 있다.

2. (법)외부서비스를 위한 웹사이트에 대해 취약점 점검을 년1회 이상 수행한다. 특히, 대외서비스를 위한 웹사이트에 대한 취약점 점검(모의해킹 등)은 반기별로 진행하여야 한다.

3. 웹사이트 취약점 점검 이후 발견된 취약점에 대한 조치현황을 정보보호관리자에게 보고한다.

4. 장비에 대한 기술적 취약점 진단 이후 발견된 취약점에 대한 조치현황을 정보보호관리자에게 보고한다.

5. 장비에 대한 기술적 취약점 진단으로 발견된 취약점에 대해 조치가 신속하게 이루어 지지 않은 건에 대해서는 조치계획을 정보보호책임자에게 보고한다.