입사 관련 업무지침

개정이력

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

목차

[목적 3](#_Toc13593542)

[범위 3](#_Toc13593543)

[제1조 (보안 서약서) 3](#_Toc13593544)

[제2조 (PC/모바일기기 보호대책) 3](#_Toc13593545)

[제3조 (업무환경 보호대책) 4](#_Toc13593546)

[제4조 (보안 위반시 조치) 5](#_Toc13593547)

[제5조 (직무변경 시 절차) 6](#_Toc13593548)

[제6조 (퇴직 시 절차) 6](#_Toc13593549)

# 목적

본 지침은 주식회사 제타큐브(이하 '회사')의 입사와 퇴사에 관한 관리 및 정보보호 위반자에 대한 징계절차 등을 정함으로써 정보보호 관리의 지속적 유지와 정보보호에 대한 경각심을 고취하는 것을 목적으로 한다.

# 범위

회사의 정보보호 관련 조직, 시스템 관리자 및 임직원에 대하여 적용된다.

# 제1조 (보안 서약서)

1. 신규 인력 채용 시 해당 임직원에 대해 정보보호서약서를 받아야 한다.

2. (법) 임직원이 회사 내 개인정보를 처리하는 경우 개인정보를 훼손/침해 또는 누설하지 않도록 하는 정보보호서약서를 받아야 한다.

3. (법) 임시직원이 회사 내 개인정보를 처리하거나 정보시스템(DB, 서버, 네트워크 등) 접근 시 정보보호서약서를 받아야 한다.

4. (법) 외부자가 회사 내 개인정보를 처리하거나 정보시스템(DB, 서버, 네트워크 등) 접근 시 정보보호서약서를 받아야 한다.

# 제2조 (PC/모바일기기 보호대책)

1. PC의 화면보호기를 30분 이상 자리 이석 시 자동으로 설정되도록 한다. 단, 모니터링 등 업무목적상 화면보호기를 실시할 수 없는 PC에 대해서는 예외로 한다.

2. 업무용으로 사용하는 모바일기기에 대한 관리는 다음을 따라야 한다.

가. 회사 자산에 정식 등록되지 않은 모바일기기(핸드폰 등 통신모듈이 자체 내장된 모바일기기 포함)를 업무용으로 사용하는 것을 원칙적으로 금한다. 단, 유지보수 등을 위해 회사 자산에 정식 등록되지 않은 모바일기기를 통제구역 및 제한구역에 반입하고자 할 경우에는 물리적보안지침을 따른다.

나. 회사의 내부망에 접속하기 위해서는 기기인증 또는 IP인증 등을 받아야 한다.

다. 회사 자산에 정식 등록된 모바일기기는 내부 네트워크에서만 사용한다.

라. 모바일기기를 통해 정보시스템에 접근하지 않는다. 다만, 업무상 필요한 경우에는 사전 승인을 거쳐 최소한의 권한으로 접근될 수 있도록 한다.

마. 회사의 문서파일을 모바일기기에 저장하지 않는다. 단, 업무상 필요에 의해 저장해야 할 경우에는 암호화하여 저장한다.

바. 모바일백신을 설치한다.

사. 모바일기기를 통한 정보시스템의 사용현황을 반기별(6개월)로 해당 정보시스템 담당자가 모니터링 후 해당 자산 책임자에게 보고한다.

# 제3조 (업무환경 보호대책)

1. 책상, 모니터, 벽면 등 개인업무 환경에 패스워드의 노출(포스트잇에 기록 부착 등)을 금지한다.

2. (법) 일정시간 동안 자리이석, 퇴근, 휴가 시 고객정보/기밀정보가 포함된 문서, 저장매체는 시건장치가 있는곳에 시건하여 보관한다.

3. 출력 실행 이후 즉각적으로 출력물을 회수한다.

4. (법) 개인정보 관련 교육자료에 개인정보가 포함된 출력물을 불법적으로 유출하면 법적 책임을 지게됨을 포함시키고 있어야 한다.

5. 사무처리기기, 문서고, 공용PC, 파일서버 등 사무실에서 공용으로 사용하는 장비는 제한구역내 배치한다.

6. 공용PC 사용 시, 패스워드가 걸리는 화면보호기를 30분으로 설정해야하며, 공용계정 사용 시 반기별로 패스워드를 변경해야 한다.

7. (법) 기밀문서를 보관하는 공용 캐비닛은 담당자와 책임자를 지정하고, 퇴근 시 잠금상태를 확인하여야 한다.

8. 파일서버 사용 시 사용자 별로 계정을 부여하고 알 필요성에 의해 최소한의 접근권한을 부여한다.

# 제4조 (보안 위반시 조치)

1. 전 임직원의 정보보호 책임과 의무사항 이행에 따라 다음과 같은 상벌규정을 적용할 수 있다.

가. 포상 규정

1) 인사고가 가점: 정보보호 책임과 의무사항에 대한 이행결과가 우수할 경우

나. 처벌 규정

1) 경고~견책조치: 대외비 정보/문서를 승인없이 외부에 유출 또는 ID대여/도용 등 단순과실 또는 판단오류로 인해 문제가 발생하였으나 회사에 불이익이 초래하지 않은 경우

2) 견책~감급조치: 대외비 정보/문서를 승인없이 외부에 유출 또는 ID대여/도용 등 단순과실 또는 판단오류로 인해 회사에 불이익이 초래한 경우

3) 감봉~징계해직: 사내 중요정보시스템의 계정을 승인없이 공유하는 등 불순한 의도가 내포된 행위가 발생되었으나 회사에 불이익이 초래하지 않은 경우

4) 강격~징계해직: 기밀 정보/문서를 승인없이 외부에 유출하는 등 불순한 의도가 내포된 행위로 인해 회사에 불이익이 초래한 경우

※ 견책: 잘못을 꾸짖고 앞으로 그런일이 없도록 주의를 주는 가장 가벼운 징계 처분

※ 감급: 보수를 줄여서 줌

※ 감봉: 일정한 기간동안 보수의 3분의 1 이하를 줄여서 줌

※ 강격: 직급을 낮춤

2. 관련 외부자가 법령, 규제 및 내부정책을 위반 시 조치관련한 내용은 SLA, 계약서 등에 명시하여야 한다.

# 제5조 (직무변경 시 절차)

1. 직무변경 시 자산반납, 접근권한 회수.조정, 결과 확인은 다음을 따른다.

가. 접근권한

1) 직무변경 시 해당 부서장은 현황을 관련 부서(정보보호 및 시스템 운영 등)에 공유한다.

2) 관련 부서(정보보호 및 시스템 운영 등)는 임직원 및 외부자의 직무변경 발생 시, 정보시스템의 접근권한을 조정한다.

3) 관련 부서(정보보호 및 시스템 운영 등)는 정보시스템 접근권한의 조정한 결과를 해당 부서장에게 공유한다.

나. 자산

1) 해당 부서장은 직무변경으로 인해 자산에 대한 사용자가 변경되었음을 자산관리담당자에게 알린다

2) 자산관리담당자는 직무변경에 맞춰서 자산을 재 할당한다.

# 제6조 (퇴직 시 절차)

1. 퇴직 시 자산반납, 접근권한 회수.조정, 결과 확인은 다음을 따른다.

가. 접근권한

1) 퇴직자 발생 시 인사부서는 현황을 관련 부서(정보보호 및 시스템 운영 등)에 공유한다.

2) 관련 부서(정보보호 및 시스템 운영 등)는 임직원 및 외부자의 퇴사자 발생 시, 정보시스템의 접근권한을 회수한다.

3) 관련 부서(정보보호 및 시스템 운영 등)는 정보시스템 접근권한의 회수한 결과를 인사부서에 공유한다.

나. 자산

1) 인사부서는 퇴직으로 인한 자산에 대한 사용자가 변경되었음을 자산관리담당자에게 알린다

2) 자산관리담당자는 사용자가 반납한 자산을 확인 후 인사부서에 공유한다.