# 정보보안 및 개인정보보호 규정

| | |
|---|---|
| 문서관리번호 | DS-정개-221201 |
| 담당자(부서) | 전상화(관리부) |

(주)다솜에스앤씨

# 제정 및 개정 이력

| 일자 | 사유 |
|---|---|
| 2022.12.01 | 최초 제정 |
| 2023.04.25 | 개인정보보호 위원회 역할 명시 |
| 2024.05.21 | 부칙 조항 개정 - 고객사 현장(SOC) 파견의 경우 추가 |

(시행일) 본 지침은 등록된 제정 및 개정 일자 이후 즉시 시행한다.

## I. 정보보호 규정

### 제1장 총칙

제1조(목적) 이 지침은 다음 각 호의 보안 관련 상위 법규를 준수하고, (주)다솜에스앤씨(이하 "회사")의 자산을 내·외부로부터의 훼손, 변조, 도난, 유출 등 다양한 형태의 위협에 효과적으로 보호하기 위해 정보 보호 정책과 임직원이 준수할 정보보호 규정을 정할 것을 목적으로 한다.

1. 개인정보 보호법

2. 정보통신망 이용 촉진 및 정보 보호에 관한 법률

3. 신용정보의 이용 및 보호에 관한 법률

4. 전자금융거래법

5. 정보통신기반 보호법

제2조(적용 범위) 이 지침은 회사에 근무하는 전 임직원을 대상으로 적용되며, 계약관계에 의하여 회사의 자산에 접근하는 모든 제 3자에게도 적용된다.

제3조(용어 정의) 이 지침에서 사용되는 용어의 정의는 다음과 같다.

1. "정보보호위원회"라 함은 회사의 IT운영 및 일반보안에 대한 의사결정을 수행하는 정보보호위원회와 개인정보에 대한 주요 의사결정을 수행하는 개인정보보호위원회를 총칭한다.

2. "정보보호담당부서"라 함은 정보보호 실무를 수행하는 정보보호 조직으로서 당사 관리부를 말한다.

3. "정보보안 책임자"란 정보보안 조직을 지휘하고 정보보안 업무를 총괄하기 위해 직제규정의 업무 분장표에 따른 업무담당 부서장을 말한다.

4. "정보보안관리자"란 정보보안 업무를 수행하기 위해 정보보안책임자가 겸직한다.

5. "시스템관리자"라 함은 각 정보시스템의 운영 및 관리를 담당하는 관리자 및 담당자를 말한다.

6. "정보보호 사고"라 함은 보호관리 대상에 속하는 정보 및 정보시스템이 무단으로 유출 또는 변조된 경우이다.

7. "정보통신망"이란「전기통신기본법」제2조 제2호에 따 파괴되거나, 유출·변조되어 업무수행에 지장을 초래하는 사고를 말한다. 다른 전기통신 설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신 하는 정보 통신체제를 말한다.

8. "정보시스템"이라 함은 회사가 보유하고 있는 컴퓨터 및 주변장치, 전산시스템, 네트워크, 소프트웨어 및 각종

영상매체시설물 등 정보를 관리하기 위해 필요한 모든 하드웨어 및 소프트웨어를 총칭한다.

9. "정보자산"이라 함은 회사가 보유하고 있는 지적재산권과 영업비밀 등 기술상, 경영상의 내용 그 자체와 이를 포함하고 있는 문서, 네트워크, 서버, 정보보호시스템, 응용프로그램, PC, 소프트웨어, 부대설비 및 기타 유무형의 모든 자산을 의미한다.

10. "제3자"라 함은 방문객, 피교육자 등 회사 임직원이 아닌 자 또는 외주용역 등 회사와 계약관계에 있는 타 회사(조직) 및 이에 속하는 직원을 지칭한다.

11. "통제구역"이라 함은 특정한 목적을 위하여 회사가 지정한 보안구역으로, 사전 허가된 인원만 제한적으로 출입할 수 있는 지역을 말한다.

제4조(책임사항) ① 정보보호담당부서는 상위 법규, 회사 정보보호 정책 및 지침에 근거한 정보보호 활동을 성실히 수행해야 한다.

② 모든 임직원 및 제3자는 정보보호담당부서 및 개인정보관리부서의 정보보호 활동에 성실히 협조해야 한다.

③정보보호담당부서는 이 지침 및 관련 지침의 타당성을 연 1회 이상 검토하여 제·개정한다.

**제2장 정보보호 대상**

제5조(정보보호 정의) ① 정보의 보호라 함은 정보의 생성, 저장, 처리, 송신, 수신 시에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 비용대비 효과적으로 방지하여 정보에 대한 가용성, 무결성, 기밀성을 확보하는 것이다.

② 회사는 정보를 보호하기 위하여 특정 정책, 지침, 절차, 조직 구조 및 소프트웨어 기능을 포함하는 적절한 범위의 통제를 수행한다.

제6조(정보보호 목표) 정보보호의 목표는 회사 업무의 연속성을 보장하고, 정보보호 사고로 인한 시스템 및 자원의 피해를 최소화하는 것이다.

제7조(정보보호 범위) ① 정보보호는 회사의 전 조직을 대상으로 한다. 정보보호 대상이 되는 회사의 자산은 다음 각 호와 같다.

1. 네트워크

2. 서버

3. 정보보호시스템

4. 응용프로그램

5. 문서

6. PC

7. 소프트웨어

8. 부대시설

9. 기타 유무형 자산

② 회사가 책임이 있거나 통제를 하고 있는 외부의 공급자나 고객과의 모든 의사소통 인터페이스를 포함하며, 회사가 고객에게 공급하여 고객 사이트에 위치한 장비 중 회사의 자산에 속하는 것은 정보보호 범위에 포함한다.

**제 3 장 정보보호조직**

제8조(정보보호위원회의 구성) ① 개인정보를 포함한 회사 전반의 정보보호에 대한 원활한 의사결정과 유관 조직과의 업무협조 및 상호 조정이 이루어지도록 정보보호위원회를 구성하여 운영한다.

② 정보보호위원회는 사안에 따라 정보보호위원회와 개인정보보호위원회로 개최될 수 있으며, 위원장인 정보보호책임자 및 개인정보보호책임자 주관 하에 운영한다.

③ 위원장은 상위 법규 요구사항 및 회사의 업무 환경을 고려하여 정보보호위원회를 구성해야 한다.

제9조(정보보호조직의 구성) ① 회사 정보자산의 보호 및 관리를 위해 정보보호담당부서와 개인정보관리부서를 중심으로 정보보호조직을 구성하여 운영한다.

② 정보보호조직의 정보보호책임자는 IT 보안 및 일반 보안업무를 총괄하고, 개인정보보호책임자는 개인정보보호 업무를 총괄한다.

③ 선임된 정보보호책임자와 개인정보보호책임자는 정보보호 실무를 수행할 정보보호관리자·담당자를 지정하고, 그 역할 및 책임을 명확히 정의하여 협업 운영하도록 한다.

④ 정보보호책임자 및 개인정보보호책임자는 임원 또는 그에 준하는 직원으로 임명한다.

제10조(정보보안 조직의 운영) 정보보안책임자는 다음 각 호의 업무를 수행하기 위하여 정보보안관리자, 시스템관리자를 지정하여 운영할 수 있다. 정보보안책임자에 부여하는 기본 활동 및 역할은 다음 각 호와 같다.

1. 정보보안 정책 및 기본계획 수립·시행

2. 정보보안 관련 규정·요령 등 제·개정

3. 보안심사위원회에 정보보안 분야 안건 심의 주관

4. 정보보안 업무 관리·감독

5. 정보통신실(전산실), 정보통신망 및 정보자료 등의 보안관리

6. 정보보안 관리실태 평가(별지 제1호)

7. 사이버공격 대응 및 조치활동

8. 정보보안 교육 및 정보협력

**제4장 정보자산 관리**

제11조(자산의 소유권 등) ① 회사의 모든 정보, 문서, 전산기기 및 서비스, 기타 자산은 회사의 중요 자산이며 회사가 그 소유권을 갖는다.

② 중요 자산은 접근과 사용에 대한 적절한 통제 절차를 수립해야 하며, 모든 회사 구성원은 회사 자산을 보호할 의무가 있다.

제12조(정보자산의 분류) ① 정보자산은 그 중요도에 따라 "비밀", "대외비", "일반"으로 분류한다.

② 정보자산의 분류는 일정 기간마다 새롭게 지정, 변경 및 해제가 가능하다.

제13조(정보자산 등급 결정) 각 정보자산의 등급은 생성 시점에 가치와 중요도에 따라 등급을 분류하여 관리한다.

제14조(정보자산의 보호) ① 정보자산은 지정된 장소에 보관되어야 하며, 이용에 대한 통제 절차를 수립해야 한다.

② 정보자산은 백업 및 복구절차를 수립하여 장애 및 재해에 대비하고 업무의 연속성을 보장해야 한다.

③ 정보보호담당부서는 정보자산에 대하여 주기적으로 위험 분석을 수행하고 보호 대책을 수립하여야 한다.

제15조(접근 권한) ① 정보자산에 대한 접근권한은 업무 수행에 필요한 최소 범위로 제한하여 관리해야 한다.

② 제3자를 포함한 모든 임직원은 자신의 업무와 무관한 정보자산에 대해 무단 접근을 시도해서는 안된다.

**제5장 인적 보안**

제16조(임직원 보안) ① 모든 임직원은 입사, 퇴사 및 연봉계약 시 정보보호서약서를 작성하여 제출해야 한다.

② 임직원은 퇴직 시 회사의 모든 정보자산 및 이에 대한 접근권한을 반환해야 한다.

③ 모든 임직원은 전출 및 직무변경 등의 사유 발생 시 신규 업무에 무관한 모든 정보자산 및 접근권한을 반환해야 할 의무가 있다.

제17조(제3자 보안) ① 제3자 및 외부인력에게 업무를 위탁하거나 회사 정보자산으로의 접근을 허용할 때에는 비밀유지 및 정보보호 제반 규정 준수에 대한 정보보호서약서를 징구해야 한다.

② 제3자는 상위 법규와 회사 정보보호 관련 정책 및 제반 지침에 따라 업무를 수행해야 하며, 다음 각호를 준수해야 한다.

1. 업무 수행 중 보안상 의심되는 문제점을 발견할 경우 지체없이 해당 관리자에게 알려야 하며, 이를 임의 오·남용해서는 안된다.

2. 업무 종료 시 회사의 모든 정보자산 및 이에 대한 접근권한을 반환해야 한다.

3. 기타 임직원의 보안 요구사항 및 절차에 성실히 협조해야 한다.

제18조(정보시스템 모니터링) ①정보보호 책임자는 개인정보의 관리 시스템 및 실태 점검을 통하여 취약점을 개선하여야 한다.

②정보보호 책임자는 개인정보 자체 점검 및 보안감사를 위한 감사 대상, 절차, 방법 등의 계획을 수립할 수 있다.

③정보보호 자체점검은 일단위로 매일 실시하며 정보보호 자체검사는 연1회 이상 실시한다.

④정보보호를 위한 모니터링 과정에서 발견된 취약점 및 보안규정 위반사항이 발견된 경우에는 적절한 조치를 취하여야 한다.

제19조(정보보호 교육) ① 모든 임직원 및 제3자가 정보보호 상위 법규 및 회사 정보보호 정책을 숙지하고, 지속적인 보안인식 제고가 이루어질 수 있도록 정기적인 보안교육을 실시해야 한다.

② 정보보호 교육은 상위 법규 요구사항을 반영하여 계획 및 구성하여 수행하고, 필요에 따라 외부 기관에 위탁하여 실시할 수 있다.

제20조(직무의 분리) ① 정보시스템 업무에 대하여 인력 운용상 가능한 범위 내에서 최대한 직무를 분리, 운영함으로써 내부 통제를 강화하고 권한 오남용을 방지한다.

② 직무의 분리는 가능한 아래 각 호의 경우를 우선적으로 분리한다.

1. 직무 실시와 승인

2. 보안감사와 시스템 운영

3. 서비스 운영과 개발

③ 직무 미분리로 인한 보안상 위해 요소가 발생하지 않도록 교육 및 관리를 강화하도록 한다

**제6장 관리적 보안**

제21조(정보보호 관련 사고 대응) ① 회사의 업무 활동을 방해하는 정보보호 관련 사고의 효율적인 처리 및 복구를 위한 대응체계를 갖추어 피해를 최소화하고, 업무수행 및 서비스 제공의 연속성을 확보한다.

② 모든 임직원은 보안 사고와 보안 체계의 약점(또는 약점으로 의심되는 것) 또는 정보시스템 장애 발생을 인지한 즉시 정보보호담당부서와 소속 부서장에게 보고할 의무가 있다.

③ 회사에 재산상의 손실 및 이미지를 훼손하는 보안 사고 발생 시에는 관련 사규에 따라 처벌하고 민·형사상 모든 손해를 청구한다.

제22조(준거성 관리) ① 회사의 모든 업무활동은 회사 내부 요구 사항과 외부 관련 법규를 준수하여 이루어져야 한다.

② 제3자를 포함한 모든 임직원이 상위 법규 및 회사 정보보호 제반 규정을 준수하고 위배하지 않도록 지속적인 감사 및 모니터링을 통해 준거성 관리를 수행해야 한다.

제23조(업무 연속성 관리) ① 재난 발생 시 최소한의 업무 수행 기능이 계속될 수 있도록 재난 복구 및 업무 연속성 계획을 수립하고 운용하여야 한다.

② 업무 프로세스의 중요한 변경 또는 환경 변화 등이 발생할 경우에 업무연속성 계획을 변경 관리하여야 한다.

③ 실제 재난 발생 시 재난 복구 계획의 유효성이 상실되지 않도록 정기적으로 유효성을 테스트하고, 보완하여야 한다.

**제7장 물리적 보안**

제24조(통제구역 지정) ① 회사 내 모든 시설은 다음 각호와 같이 그 성격에 따라 일반구역·보호구역·통제구역으로 분류하여 관리한다.

1. 통제구역: 전산실 등 중요 정보가 보관되거나 처리되는 지역으로 비인가자의 출입이 금지되는 보안상 극히 중요한 구역을 말한다.

2. 보호구역: 비인가자의 출입이 제한되어야 할 구역으로 통제구역과 일반영역을 제외한 회사 모든 영역을 말한다.

3. 일반구역: 회사와 관련된 모든 인력이 자유롭게 출입 가능한 구역으로 통제구역과 보호구역을 제외한 접견실과 같은 영역을 말한다.

② 분류 지정된 구역의 특성에 따라 비인가자의 접근과 손상을 예방할 수 있도록 적절한 보호조치를 수립 및 적용하여 관리해야 한다.

③ 중요정보가 보관되거나 처리되는 지역은 사전에 통제구역으로 설정하며, 통제구역은 별도의 관리책임자를 지정하여 관리한다.

제25조(출입통제 관리) ① 모든 임직원은 사옥 내에서 반드시 사원증을 패용하여야 하며, 허가된 지역에 한하여 출입하도록 한다.

② 출입증은 본인만이 사용하여야 하며, 타인에게 대여하거나 타인의 출입증을 사용해서는 안된다.

③ 내방객과의 업무는 접견실 또는 사무실 이외의 별도 지정된 장소를 이용함을 원칙으로 한다.

④ 업무 상 제3자의 사무실 출입이 필요한 경우 발급된 출입증 패용 후 임직원의 동행 하에 허가된 지역에 한하여 출입이 허용될 수 있도록 제한해야 한다.

제26조(정보시스템 기기 보안 관리) 정보시스템 기기들은 화재, 홍수, 지진, 폭발, 전쟁 또는 다른 형태의 자연 재해 및 인재로부터 발생되는 피해를 보호하기 위해 물리적인 보호 방안이 설계되고 적용되는 장소에 설치되어야 하고, 비인가된 접근과 기타 위해 요소로부터 보호될 수 있는 곳에 위치하도록 한다.

제27조(사무환경 보안) ① 문서함 등 모든 사무집기는 사용자 책임으로 시건을 철저히 하여 정보의 부당한 유출

을 방지하여야 한다.

② 사무환경의 보안성 제고를 위하여 취약장소, 시설, 설비 등에 대한 대책을 강구 및 시행하여야 한다.

제28조(반출입 관리) ① 제3자를 포함한 모든 임직원은 회사의 모든 정보자산을 임의로 반출해서는 안된다.

② 회사 정보자산의 유출, 훼손 및 도난을 방지하기 위한 규정을 마련하고, 이를 준수하여 반출입 관리를 수행해야 한다.

**제8장 정보시스템 보안**

제29조(운영 절차 및 책임) ① 정보보호담당자는 정보시스템의 보안 운영 절차를 문서화하여 관리한다.

② 정보시스템 기기, 응용 소프트웨어, 운영 프로그램의 변경 통제에 대한 절차를 규정하고 준수한다.

③ 정보시스템의 오류, 서비스의 중단, 서비스 거부, 불완전한 데이터로 야기되는 오류, 비밀성 침해 등이 발생할 경우 사고 처리를 위한 절차를 규정하고 준수한다.

제30조(개발보안) ① 개발시스템 및 운영시스템은 분리한다.

② 프로그램 개발 및 테스트 행위는 운용시스템과 분리되어 이루어져야 하며, 운용시스템 이관 전에 충분한 테스트 및 관리자의 승인을 득하여 적용한다.

③ 응용프로그램은 분석, 설계, 구현, 테스트, 이관 각각의 개발 단계별로 보안성을 고려하여야 한다.

제31조(시스템 계획) 적절한 저장 능력 및 정보처리 능력을 가질 수 있도록 시스템의 처리속도와 사용 용량에 대하여 주기적으로 모니터링을 실시하고 이를 기록·관리해야 한다.

제32조(네트워크 모니터링) 네트워크 서비스 장애 및 보안사고 방지를 위해 네트워크 트래픽 모니터링을 수행하고, 이상징후 발견 시 정보보호담당부서 및 상위 부서장에게 보고하여 신속하게 조치될 수 있도록 해야 한다.

제33조(시스템 유지 관리) ① 중요한 정보와 소프트웨어에 대한 백업 계획을 수립하고 백업 및 복구 테스트를 주기적으로 수행해야 한다.

② 주요 시스템의 접근 및 운영로그를 로깅하여 보관·관리하고, 이를 주기적으로 검토해야 한다.

제34조(저장 매체 폐기) ① 회사 소유의 저장 매체를 폐기할 경우 저장내용을 식별할 수 없도록 소각·물리적 완전파쇄·전자기장 소거 등의 방법을 사용하여 폐기한다.

② 컴퓨터 시스템을 회수 또는 용도 변경하여 재사용하고자 할 때에는 그 시스템의 기억 장치 내에 있는 모든 자료를 복구 불가능하도록 완전 삭제해야 한다.

제35조(정보 취급 및 보안) 회사가 소유 또는 관리하는 정보 자산에 대한 비인가된 접근, 폭로 및 오용을 방지하기 위해 정보 자산 등급별 처리 기준을 수립하여 관리해야 한다.

제36조(시스템 관련 문서의 보안) 시스템 운영 문서는 비인가된 접근으로부터 보호하기 위하여 물리적으로 안전한 장소에 보관하고, 전자적 형태의 파일의 경우 접근통제를 실시하여 인가된 사람만이 접근할 수 있도록 조치해야 한다.

제37조(인터넷 보안) ① 전자거래시스템 등과 같이 인터넷 기반의 서비스를 이용할 경우 정보의 변조·공개·거래부인과 같은 위협으로부터 보호받을 수 있는 통제대책을 마련하여 적용해야 한다.

② 개인용컴퓨터(PC) 등에서 음란, 도박 등 업무와 무관한 인터넷 사이트 접근에 대한 통제대책을 수립·운영해야 한다.

제38조(사용자 인증) ① 정보시스템을 사용하는 모든 사용자는 각 개인별 고유한 ID와 PASSWORD를 통해 인증 후 사용해야 한다.

② 모든 사용자는 자신의 ID/PASSWORD가 노출되지 않도록 관리할 책임을 가지며, 노출이 의심되는 경우에는 즉시 변경 또는 변경을 요청해야 한다.

**제9장 접근 통제**

제39조(접근 통제 정책) ① 회사 정보자산의 비인가적인 침해를 방지하기 위하여 정보자산 등급에 따른 접근통제 정책을 마련해야 한다.

② 모든 정보시스템은 반드시 적절한 사용자 인증방안을 적용하여 이용하도록 한다.

제40조(네트워크 분리) ① 네트워크상의 정보와 기반 구조를 보호하기 위하여 네트워크에 대한 접근은 통제되어야 한다.

② 업무 특성 및 서비스 민감도에 따라 주요 데이터베이스 서버와 웹 서버는 보안시스템으로 분리 운영해야 한다.

제41조(운영체제 접근 제어) ① 정보보호 측면에서 필요할 경우 단말기 식별기능(IP Address에 의한 통제 등)을 적용하여 특정 위치에서의 연결만을 허용한다.

② 회사 모든 시스템의 계정 및 패스워드는 관련 기준에 따라 설정 운영되어야 한다.

제42조(이동 컴퓨팅(Mobile Computing)) 노트북 등과 같은 휴대용 정보시스템을 사용하는 사용자는 분실, 도난 및 비인가자의 시스템 접근을 방지를 위해 회사 보안기준을 준수하고, 필요한 보호조치를 취해야 한다.

제43조(외부 접속 제한) ① 외부에서 내부로의 접근 통로는 필요한 경우에만 허용하고 기본적으로는 차단한다.

② 외부에서 당사 시스템에 접속할 경우에는 인가된 사용자라도 정당한 인증 절차를 거쳐 사용하도록 한다.

③ 외부에서의 접속 통로는 외부 해킹에 대비해 사전에 안전한 보안솔루션을 적용하여 적절한 보호 대책을 취한 후 허용해야 한다.

**제10장 개인 보안**

제44조(패스워드 설정) 회사에서 사용되는 모든 컴퓨터는 부팅 패스워드·로그온 패스워드·화면보호기 패스워드를 설정하여 비인가자가 접근 및 오·남용할 수 없도록 해야 한다.

제45조(불법 소프트웨어 금지) ① 모든 소프트웨어의 소유권은 회사가 가지며, 불법적으로 사용할 용도로 복제해서는 안된다.

② 임의 복제된 불법 소프트웨어는 회사에서 사용할 수 없다.

③ 개인이 구매한 소프트웨어는 그것이 정품이라 해도 회사에서 사용할 수 없다.

제46조(바이러스 대비) ① 회사에서 사용되는 모든 저장매체는 사용 전 바이러스 검사를 수행해야 하며, 바이러스가 발견되었을 경우 즉시 정보보호담당부서에 통보하여 조치를 취하도록 한다.

② PC, 서버 등 전산기기는 바이러스에 대비하기 위해 항상 최신 백신을 유지해야 한다.

제47조(책상 정리 등) ① 퇴근이나 장기 출타 시 중요한 회사의 대외비 또는 기밀 사항을 담고 있는 문서는 책상 위 등에 방치되어서는 안되며, 시건 장치가 부착된 문서 보관함에 보관해야 한다.

② 패스워드가 설정된 화면보호기를 사용하여 PC를 사용하지 않는 경우 자동으로 화면이 잠기도록 하여야 한다. PC 사용을 재개할 때는 다시 패스워드를 입력하고 사용하도록 해야 한다.

제49조(정보보호의 날) ① 회사는 매월 정보보호의 날을 지정·시행한다.

② 임직원은 정보보호의 날에 다음 각 호에 해당하는 업무를 수행하고, 정보보호조직은 이를 점검할 수 있다.

1. 부서 정보보호 점검사항 확인
2. 생활보안 수칙 숙지

**부칙**

제1조(적용방법) 회사의 임직원이 고객사 지정장소(보안통제구역, SOC를 포함한다)에서 업무를 수행하는 경우, 고객사의 정보보호규정을 적용할 수 있다.

**정보보안 체크리스트**

| 구분 | 항목 | 점검결과 |
|---|---|---|
| 정보보안 기본활동 | 사이버보안진단의 날을 내실 있게 수행하는가? | Y/N |
| | 보직변경 등 인사이동시 정보시스템 접근권한을 신속하게 조정하는가? | Y/N |
| | 개인정보처리방침을 명문화하여 공개하고 있는가 | Y/N |
| PC 및 서버 보안관리 | 서버 PC 등 정보시스템 현황을 제대로 파악하는가? | Y/N |
| | PC 서버에 설치된 운영체제 및 응용프로그램을 최신 보안 업데이트 하였는가 | Y/N |
| | 비인가자 접근 방지를 위해 PC 부팅 비밀번호를 설정하였는가 | Y/N |
| 네트워크 보안관리 | 정보시스템 세부 구성도(IP 포함)를 최신으로 유지하면서 대외비 이상 비밀로 관리하고 있는가 | Y/N |
| | 스위치・라우터 등 네트워크 장비와 서버는 비인가자가 접속 못하도록 IP ・ MAC 통제 등 보안설정하고 불필요한 서비스포트를 제거하는가 | Y/N |
| | 시스템 최초 설치 시 등록된 관리자계정(기업명 등)・패스워드를 변경하였는가 | Y/N |
| 보안관제 등 해킹 대응활동 | 사이버공격에 대응하기 위한 관제센터를 운영하거나 同 업무를 他기관에 위탁하였는가 | Y/N |
| | 해킹메일 대응방안 등 침해사고 대응절차 등을 보안교육을 수행하는가 | Y/N |
| | 보안관제시스템에 대한 물리적인 보안대책을 준수하고 있는가? | Y/N |

(점검결과에 대한 처리방안)

- 점검결과가 "N"인 항목에 대하여 시정조치 계획을 수립하여 조치 후 결과 관리한다. 단, 임직원이 고객사의 지정장소에서 근무하는 경우 고객사의 정보보안 체크리스트를 준용하여 점검한다.

## II. 개인정보보호 규정

### 제1장 총칙

제1조(목적) 이 규정은 개인정보보호법, 정보통신망 이용 촉진 및 정보 보호에 관한 법률, 정보통신기반 보호법 등 정보보안 관련 법규를 준수하고, 고객의 개인정보를 오남용, 훼손, 변조, 유출 등으로부터 효과적으로 보호하기 위해 필요한 세부사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 규정은 회사의 전체 임직원을 대상으로 하며, 계약관계에 의하여 회사의 정보자산에 접근하는 모든 제3자에게도 적용된다.

제3조(용어정의) 이 규정에서 사용되는 용어의 정의는 다음과 같다.

1. "개인정보"란 살아있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.

①성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

②해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

③①항 또는 ②항을 제 1호의 2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다.)

1-1. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

2. "개인정보 처리"란 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

3. "정보주체"란 처리되는 정보에 의해 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

4. "개인정보 보호책임자"란 감독원의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서, 시행령 제 32조제2항에 해당하는 자를 말한다.

5. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

제4조(개인정보 보호 원칙) 회사의 임직원은 다음 각 호의 개인정보 보호원칙을 준수하여야 한다.

1. 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고, 그 목적에 필요한 범위에서 최소한의 개인정보 만을 적법하고 정당하게 수집하여야 한다.

2. 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니된다.

3. 개인정보처리자는 개인정보 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

4. 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해 받을 가능성과 그 위험정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

5. 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

6. 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

7. 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.

8. 보호법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

**제2장 개인정보 보호 조직**

제5조(개인정보 보호책임자의 의무) ①보안담당자는 고객의 개인정보보호 업무를 총괄하며 다음의 기능을 수행한다.

1. 고객 개인정보 보호를 위한 정책 수립

2. 고객 개인정보 유출 방지를 위한 내부관리시스템 구축

3. 고객정보 유출 등의 사고 발생시 지체없이 적극적인 피해구제

4. 개인정보보호에 대한 전사차원의 교육을 진행

5. 고객개인정보보를 위한 지속적인 모니터링 및 모의 훈련 계획 및 시행

6. 기타 개인정보 보호를 위하여 필요하다고 판단되는 사항

제6조(개인정보취급자의 의무) ①개인정보취급자는 개인정보 보호법, 시행령, 시행규칙 및 개인정보 보호 원칙을 준수하여야 한다.

②개인정보 유출 사실을 인지하게 된 경우, 지체없이 부서장 및 개인정보 보호책임자에게 보고하여야 한다.

③개인정보 보호 책임자가 주관하는 보호 관련 교육을 이수하고 보안서약서에 서명하여야 한다.

**제3장 개인정보 주체의 권리 보장**

제7조(개인정보 주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

1. 개인정보의 처리에 관한 정보를 제공받을 권리

2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리

3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급 포함)을 요구할 권리

4. 개인정보의 처리 정지, 정정 · 삭제 및 파기를 요구할 권리

5. 개인정보 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

제8조(개인정보의 열람) 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

제9조(개인정보의 정정·삭제) ①자신의 개인정보를 열람한 정보주체는 개인정보 처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.

②개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정 · 삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

제10조(개인정보의 파기) ①개인정보처리자는 보유기관의 경과, 개인정보의 처리 목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

②개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

**제4장 개인정보의 안전한 관리**

제11조(안전조치의무) 개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다.

제12조(보안지침) ①모든 임직원은 입사, 퇴사 및 연봉계약 시 정보보호서약서를 작성하여 제출해야 한다.

②제3자에게 업무를 위탁하거나 회사 정보자산으로의 접근을 허용할 때에는 비밀유지 및 정보보호 제반 규정 준수에 대한 정보보호서약서를 징구하여야 한다.

③회사 내 모든 시설은 그 성격에 따라 일반구역·보호구역·통제구역으로 분류하여 관리한다

④제3자를 포함한 모든 임직원은 회사의 모든 정보자산을 임의로 반출해서는 아니된다.

⑤네트워크 트래픽 모니터링을 수행하고, 이상징후 발견 시 개인정보보호책임자 등에게 보고하여 신속하게 조치될 수 있도록 한다.

⑥개인정보는 사전에 인가된 목적으로만 사용되어야 하며, 용도 외의 임의 목적으로 방치되거나 부당하게 유출되지 않도록 그 생산, 유통, 보관, 폐기 등의 전 과정을 철저히 관리하여야 한다.

**제5장 보안사고**

제13조(개인정보 유출) 개인정보의 유출은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우

2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우

3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우

4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

제14조(개인정보 유출 통지) ①개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 개인정보 보호 책

임자에게 즉시 보고하여야 하며, 개인정보 보호 책임자는 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

②개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검 보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 그로부터 5일 이내에 정보주체에게 알릴 수 있다.

1. 유출된 개인정보의 항목

2. 유출된 시점과 그 경위

3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보

4. 개인정보처리자의 대응조치 및 피해구제절차

5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

③개인정보처리자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실

2. 제1항의 통지항목 중 확인된 사항

④개인정보처리자는 개인정보 유출 사고를 인지하지 못해 유출사고가 발생한 시점으로부터 5일 이내에 해당정보주체에게 개인정보 유출 통지를 하지 아니한 경우에는 실제 유출 사고를 알게 된 시점을 입증하여야 한다.

## 제6장 보안 점검 및 교육

제15조(시스템 모니터링) ①개인정보보호 책임자는 개인정보의 관리 시스템 및 실태 점검을 통하여 취약점을 개선하여야 한다.

②개인정보보호 책임자는 개인정보 자체 점검 및 보안감사를 위한 감사 대상, 절차, 방법 등의 계획을 수립할 수 있다.

③개인정보보호 자체점검은 일단위로 매일 실시하며 개인정보보호 자체검사는 연1회 이상 실시한다.

④개인정보보호를 위한 모니터링 과정에서 발견된 취약점 및 보안규정 위반사항이 발견된 경우에는 적절한 조치를 취하여야 한다.

제16조(개인정보보호 교육) 개인정보보호 책임자는 고객의 개인정보 유출 등의 사고를 예방하기 위하여 필요한 교육을 계획하고 시행하여야 한다.

**부 칙**

제1조(적용방법) 회사의 임직원이 고객사 지정장소(보안통제구역, SOC를 포함한다)에서 업무를 수행하는 경우, 고객사의 개인정보보호규정을 적용할 수 있다.

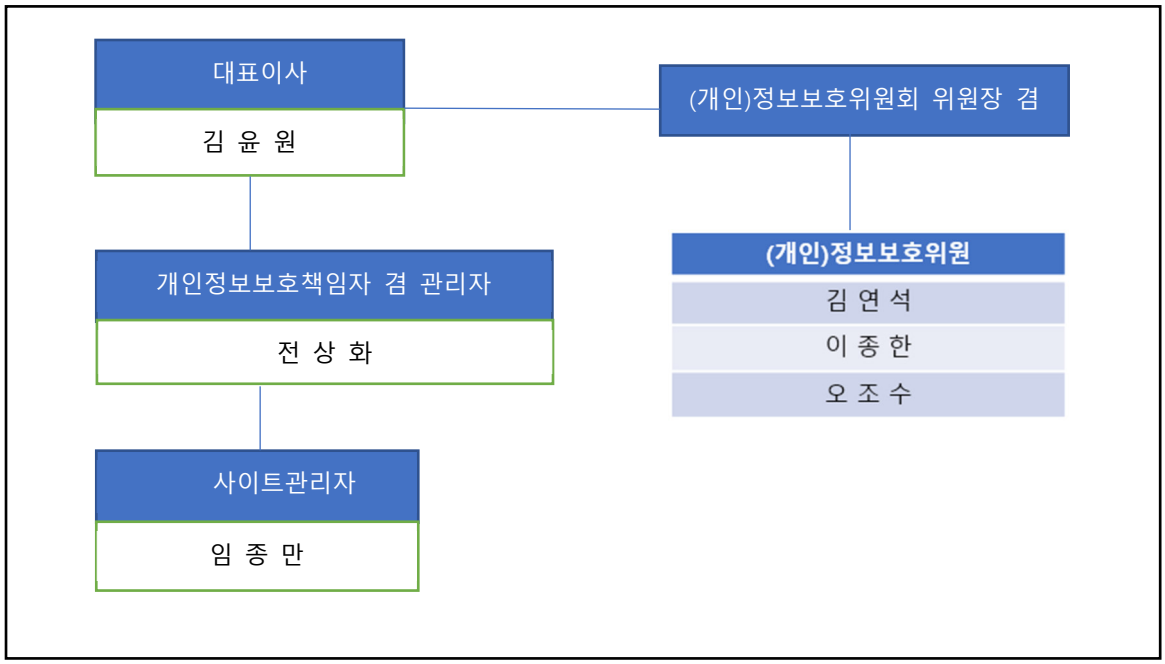
**개인정보보호 체크리스트**

| 구분 | 항목 | 답변 |
|---|---|---|
| **관계법률 및 법령 준수** | 관련 법률 및 법령 등을 준수하여 개인정보를 수집하고 있는가 | Y/N |
| | 개인정보처리방침 등 필수 고지사항을 정보주체에게 고지하고 동의를 얻었는가 | Y/N |
| | 개인정보처리방침을 명문화하여 공개하고 있는가 | Y/N |
| **개인정보 취급** | 개인정보 목적 외 제공 시 암호화 등의 조치를 하고 있는가 | Y/N |
| | 개인정보 보관 시 암호화 등의 보안조치가 있는가 | Y/N |
| | 불필요하거나 보유기간이 경과된 개인정보를 파기하였는가 | Y/N |
| **개인정보 위탁** | 개인정보 위탁 시 위탁계약서를 작성하였는가 | Y/N |
| | 개인정보 위탁 시 그 내용 및 수탁자를 정보주체에게 고지하였는가 | Y/N |
| | 연 1회 이상 수탁자 대상으로 개인정보보안 교육을 수행하는가 | Y/N |
| **보안지침** | 개인정보에 대하여 접속기록을 보관하고 점검하고 있는가 | Y/N |
| | 제3자 및 모든 임직원은 정보보안 서약서를 작성하였는가 | Y/N |
| | 개인정보에 접근권한을 최소화하고 있는가 | Y/N |
| **점검 및 교육** | 개인정보 보호를 위한 모니터링을 정기적으로 시행하고 있는가 | Y/N |
| | 접근통제시스템을 운영하고 있는가 | Y/N |
| | 개인정보취급자에 대하여 정기적인 교육을 실시하고 있는가 | Y/N |

(점검결과에 대한 처리방안)

- 점검결과가 "N"인 항목에 대하여 시정조치 계획을 수립하여 조치 후 결과 관리한다. 단, 임직원이 고객사의 지정장소에서 근무하는 경우 고객사의 개인정보보호 체크리스트를 준용하여 점검한다.

**정보보안 및 개인정보보호 조직**




**개인정보보호 위원회 명부 및 역할**

| 위원회 | 담당자 | 역할 |
|---|---|---|
| **위원장** | 김윤원 | 개인정보보호 위원회 총괄, 개인정보보호 정책 의결 및 총괄 관리 |
| **책임자** | 전상화 | 개인정보보호 위원회 책임자, 개인정보보 방침 수립 및 집행 관리 |
| **위원** | 김연석 | 개인정보보호 위원회 위원, 개인정보보호 실무 담당 |
| **위원** | 이종한 | 개인정보보호 위원회 위원, 개인정보보호 실무 담당 |
| **위원** | 오조수 | 개인정보보호 위원회 위원, 개인정보보호 실무 담당 |
| **사이트관리** | 임종만 | 개인정보보호 의결 내용 대내외 공표, 홈페이지 게시 |

**연간 보안감사 계획**

| 구분 | | 내용 | 방법 | 일자 | 대상 |
|---|---|---|---|---|---|
| 정기 모니터링 | 3월 | 정보보안 규정 준수 체크리스트 점검 | 현장방문 | 불시 | 본사 및 파견 임직원 |
| | 6월 | 개인정보보호 규정 체크리스트 점검 | 현장방문 | 불시 | |
| | 9월 | 정보보안 규정 준수 체크리스트 점검 | 현장방문 | 불시 | |
| | 12월 | 개인정보보호 규정 체크리스트 점검 | 현장방문 | 불시 | |
| 정보교육 | | 개인정보보호법 교육 | 온라인 | 불시 | 모든 임직원 |
| 중점사항 | | . 주민번호등 개인정보 개인 PC 저장금지, 퇴근 시 문서보안 관리 철저 | | | |

(보안감사 적용방법)

임직원이 고객사의 지정장소에 근무하고 지정장소가 보안통제실(SOC)인 경우 연간 보안감사 일정과 내용은 고객사의 방침을 따른다.