| 분류번호 | G - 3 | 보안 정책서 | 제, 개정일자 | 2021.08.01 |
|---|---|---|---|---|
| 관리부서 | IT | | 버전 | Version 1.1 |

# 보안 정책서

**시행일 : 2021년 5월 1일**

**동성화인텍**

# 제 · 개정 이력

| 제 · 개정 번호 | 개정 페이지 및 내용 | 제 · 개정 일자 |
|---|---|---|
| Version 1.0 | 최초 제정 | 2021.05.01 |
| Version 1.1 | 개정 | 2021.08.01 |
| | | |
| | | |
| | | |

# 목 차

# 제 1 장 총칙

제1조(목적)

본 정책은 동성화인텍(이하 "회사"라 한다)의 정보자산, 보안사항, 영업비밀 및 기타 지적재산권 등을 관리하고 보호하는데 필요한 사항을 규정하고, 나아가 회사의 경영목표 및 보안정책과 일관성을 유지할 수 있도록 노력함을 목적으로 한다.

제2조(적용범위)

본 정책은 회사 임직원 및 외부 협력업체와 파트너, 기타 회사를 출입하는 모든 사람에게 적용한다.

제3조(정의)

본 정책에서 사용되는 용어의 정의는 다음과 같다. 각종 보안관련지침도 본 정의를 준용한다.

1. "정보" 라 함은 회사의 경영 또는 활동에 필요한 일체의 지식을 말한다.
2. "정보시스템" 이라 함은 회사가 보유하고 있는 컴퓨터, 전산시스템, 네트워크, 소프트웨어 및 각종 영상매체시설물 등 정보를 관리하는데 필요한 모든 자산을 말한다.
3. "정보자산" 이라 함은 정보와 정보시스템을 포괄한 개념을 말한다.
4. "영업비밀" 이라 함은 회사가 보유 또는 보유할 정보로서 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로, 비밀로 유지된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 말하며, "1급 비밀", "2급 비밀", "대외비"로 분류한다.
5. "지적재산권" 이란 인간의 창조적 활동 도는 경험 등에 의하여 창출되거나 발견된 지식, 정보, 기술, 사상이나 감정의 표현, 영업이나 물건의 표시, 생물의 품종이나 유전자원, 그 밖에 무형적인 것으로서 재산적 가치가 실현될 수 있는 것에 관한 권리를 말한다.
6. "임직원" 이란 회사에 재직하는 임원과 직원을 말한다.
7. "외부인" 이란 회사의 임직원이 아닌 자로서 특정한 업무수행을 위해 계약관계를 체결한 자 또는 그러한 업체에 소속된 인원을 말한다.

제4조(보안선언)

1. 정보와 정보시스템 및 이에 의해 제공되는 정보서비스는 회사의 중요한 자산이다.
2. 이러한 정보자산은 그 가치와 중요성에 따라 회사 내 · 외부의 각종 위협으로부터 보호되어야 한다.
3. 회사의 모든 임직원은 본 정책을 이해하고 준수함으로써 회사의 정보자산을 보호할 책임

이 있다.

제5조(준용)

회사의 정보자산에 대한 관리는 본 정책에 따라 처리하며, 이에 명시되지 않은 사항은 관련 법령 및 회사규정이 정하는 바에 따른다.

## 제2장 보안 대상 및 조직

제6조(보안대상 및 기준)

보안의 대상이 되는 정보자산은 "정보와 정보시스템"을 포괄한 개념을 의미하며, 이를 운영하기 위한 서비스 또한 보안의 대상이 된다.

제7조(보안대상 자산기준)

회사의 보안대상이 되는 정보자산은 다음과 같은 기준에 적합하여야 한다.

1. 비밀성(Confidentiality): 정보의 소유자가 원하는 대로 정보의 비밀이 유지되어야 하며, 권한이 없는 사람에게 함부로 공개되지 않아야 한다.
2. 무결성(Integrity): 비인가된 자에 의한 정보의 변경, 삭제, 생성 등으로부터 보호하여 정보의 정확성과 완전성이 보장되어야 한다.
3. 가용성(Availability): 정보시스템은 적절한 방법으로 작동되어야 하며, 정당한 방법으로 권한이 주어진 사용자에게 정보 서비스를 거부하지 않아야 한다.
4. 준거성(Compliance): 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 부정경쟁방지 및 영업비밀 보호에 관한 법률 등 관련 법률의 요구사항을 준수하여야 한다.

제8조(보안 기능)

정보자산에 대한 보안 필요성을 충족시키기 위해서는 다음과 같은 보안기능이 존재하여야 한다.

1. 식별 및 확인: 내 · 외부인을 막론하고 정보자산에 접근하고자 하는 자에 대해 식별하고 확인하여야 한다.
2. 권한 부여 및 삭제: 정보자산을 업무의 성격 및 중요도에 따라 구분하고, 이에 따른 사용자 권한을 부여하고 관리하여야 한다.
3. 접근통제: 회사 주요시설 등 중요 정보자산에 대한 접근을 통제하여야 한다.
4. 책임 부여 및 추적: 정보자산의 관련자들에 대해서 의무와 책임을 명확히 하고, 정보의 유출 등 사건 발생시 책임을 추적할 수 있어야 한다.
5. 기타: 정보자산에 대해 제7조(보안대상 자산기준)의 기준에 적합한 기능이 제공되고 관리되어야 한다.

제9조(보안 조직)

1. 정보자산의 관리는 각 팀 단위로 하는 것을 원칙으로 하며 이를 효과적으로 보호하기 위한 역할과 책임은 모든 사용자에게 있다.

2. 보안조직에 대한 상세 사항은 '보안조직관리지침'에 따른다.

## 제3장 정보문서의 관리

제10조(정보문서의 분류)

1. 회사의 정보 문서는 가치와 중요도에 따라 "영업비밀"과 "일반"으로 분류, 관리한다.

2. "영업비밀" 은 "1급비밀", "2급비밀", "대외비"로 분류, 관리하며 "영업비밀보호규정 제7조(영업비밀의 등급 및 분류기준)" 조문을 준용한다.

3. "일반(Public)"이란 "영업비밀"이 아닌 그 이외의 정보 문서를 말한다. 또는 "대외비"가 아닌 그 이외의 정보 문서를 말한다.

4. 정보 문서의 등급 분류는 일정 기간마다 새롭게 지정, 변경 및 해제가 가능하다.

제11조(정보문서의 등급의 결정)

각 정보 문서의 등급은 정보의 생성 시점에 소유자가 부여한다. 부여시에는 정보를 적절하게 보호할 수 있도록 과대 또는 과소 분류되지 않도록 주의해야 한다.

제12조(정보문서의 관리)

정보문서의 관리에 대한 상세 사항은 '비밀문서관리규칙' 에 따른다.

## 제4장 인적 보안

제13조(보안준수)

1. 모든 임직원, 협력업체 직원은 본 정책을 포함한 보안과 관련된 정책, 지침, 절차 등을 준수해야 하며, 이를 위반할 경우 사안의 경중에 따라 징계할 수 있다.

2. 임직원 등 개인의 보안준수에 대한 상세 사항과 보안 사고처리 절차 및 징계에 대해서는 '개인보안지침'에 따른다.

제14조(보안서약서 작성)

모든 임직원의 입 · 퇴사시와 연봉계약시 보안서약서를 작성하여야 한다. 이때 보안서약서는

"영업비밀보호규정" 제23조에 따라 징구한다.

제15조(보안교육)

1. 보안관리자는 모든 임직원 입사시 사내 보안교육을 받도록 한다.

2. 관리책임자는 모든 임직원을 대상으로 년 1회 이상 보안교육 실시를 주관한다.

3. 보안교육은 외부 전문 업체에 위탁 실시할 수 있다.

제16조(퇴직관리)

전 임직원은 퇴직, 전출 또는 직무의 변경이 발생하는 경우 소지하고 있는 모든 정보자산을 반환하여야 한다.

## 제5장 물리적 보안

제17조(시설관리)

회사의 모든 시설에는 일반인의 접근을 방지하기 위해 출입통제장치를 설치하며 각 출입통제장치에는 담당자를 지정하여 관리한다.

제18조(장비관리)

정보시스템 및 관련 장비를 보안관련 각종 위협으로부터 물리적으로 보호하기 위해 다음 사항이 준수되어야 한다.

1. 장비의 설치 및 보호: 장비의 설치 시에는 내 · 외부인의 불필요한 접근을 막기 위해 필요한 통제수단을 강구하여야 한다. 또한 특별한 관리가 필요한 장비는 별도로 관리하여야 한다.

2. 장비의 반출: 장비가 외부로 반출되거나 반입되는 경우 보안담당자의 승인을 받아야 한다. (단, 사업장간 및 그룹사간 이동 시 예외)

제19조(통제구역)

회사 내 중요설비를 보호하기 위해 물리적 통제구역을 설정하고 관리책임자를 지정하여 필요한 보안대책을 강구한다. 또한 소수의 인가된 임직원만이 출입할 수 있도록 출입을 통제하고, 이들에 대한 출입권한을 정기적으로 검토하여 갱신해야 한다.

제20조(일반구역)

사무실 등 일반구역에서의 정보유출을 방지하기 위하여 임직원들은 자리 이석 시 책상에 중요문서를 놓지 않아야 하며, 컴퓨터의 화면에 중요 정보가 남아있지 않아야 한다. 또한 일정시간 이상 자리 이석 시 화면보호기를 작동시켜야 한다.

제21조(기타 물리적 보안) 물리적 보안에 대한 상세 사항은 '물리적보안지침' 에 따른다.

## 제6장 정보시스템 보안

제22조(정보시스템 보안관리)

1. 정보자산의 비밀성, 무결성, 가용성 확보를 위해 보안책임자는 모든 정보시스템에 대한

운영 및 관리절차를 수립하고, 이에 따라 관리담당자를 지정하여 관리하도록 조치하여야 한다.

2. 정보시스템 보안관리에 대한 상세 사항은 '정보시스템관리지침' 에 따른다.

제23조(컴퓨터 보안관리)

1. 회사 내 모든 컴퓨터 사용자는 정보자산이 도난 또는 파괴되거나, 불법적으로 유출, 변경, 파괴되지 않도록 해야 한다.

2. 컴퓨터 보안관리에 대한 상세 사항은 'PC정보보안지침'에 따른다.

제24조(서버 보안관리)

1. 회사의 정보시스템을 구성하는 모든 서버들에 대해 적절한 보안관리 및 통제방안을 수립하여 관리하여야 한다.

2. 서버 보안관리에 대한 상세 사항은 '서버정보보안지침' 에 따른다.

제25조(네트워크 보안관리)

1. 네트워크상의 정보 등을 보호하기 위하여 보안책임자는 별도의 담당자를 임명하고 적절한 보안관리 및 통제방안을 수립하여 관리하여야 한다.

2. 네트워크 보안관리에 대한 상세 사항은 '네트워크정보보안지침' 에 따른다.

제26조(데이터베이스 보안관리)

1. 데이터의 비밀성, 안전성, 신뢰성을 위해 데이터베이스 관리자와 개발자들은 데이터베이스 구축하고 관리하여야 한다.

2. 데이터베이스 보안관리에 대한 상세 사항은 '데이터베이스정보보안지침' 에 따른다.

제27조(응용시스템 보안관리)

1. 응용시스템의 구축 및 관리 시 응용시스템의 비밀성, 안전성, 신뢰성을 확보하고 관리하여야 한다.

2. 응용시스템 보안관리에 대한 상세 사항은 '응용시스템정보보안지침' 에 따른다.

## 제7장 기타 보안 관리

제28조(보안점검)

1. 회사는 년 2회 이상 정기적으로 임직원과 각 부서를 대상으로 보안점검을 실시하여야 하며, 필요시 특정 임직원 및 부서를 선정하여 불시에 점검할 수 있다.

2. 보안점검에 대한 상세 사항은 '개인보안지침' 에 따른다.

제29조(보안점검계획 수립)

1. 매년 보안점검계획을 수립하여 관리책임자의 승인을 얻은 후 시행한다.
2. 보안계획을 수립하기 전에 회사의 보안 요구사항을 파악하고, 내 · 외부의 보안위협 및 취약점에 대한 대응책 수립을 위해 외부 전문가를 활용 위험평가 업무를 수행할 수 있다.

제30조(보안진단)

보안관리자는 관리책임자의 지시가 있거나, 보안진단계획에 의거하여 정보보안 정책 및 지침의 준수 여부와 적용된 정보보안 대책의 적합성을 검토하고 이를 경영진에게 보고할 수 있다. 필요시 외부 전문 업체에 위탁하여 보안진단을 실시할 수 있다.

제31조(법규준수)

보안 업무를 수행함에 있어 국내 관련 법규를 준수하여야 한다.

## 부칙

제1조(시행일)

본 정책은 공표된 날로부터 시행한다.