기술보호규정

2022. 12. 23

바이오에프디엔씨

BIO-FD&C
Life Science for Happiness
(주)바이오에프디엔씨

제 1 장 총 칙

제 1 조【목 적】

본 규정은 주식회사 바이오에프디엔씨(이하 "회사"라 한다)의 정보자산, 보안사항, 영업비밀 및 기타 지식재산권 등을 관리하고 보호하는데 필요한 사항을 규정하고, 나아가 회사의 경영목표 및 보안정책과 일 관성을 유지할 수 있도록 노력함을 목적으로 한다.

제 2 조【적용범위】

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

제 3 조【보안선언】

본 정책에서 사용하는 용어의 정의는 다음과 같다.

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 책임이 있다.

제 4 조【준 용】

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

제 2 장 보안대상 및 조직

제 5 조【보안대상】

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

① "정보"는 회사 경영과 관련하여 수집한 자료를 실제 상황에 도움이 될 수 있도록 정리한 자료를 의미하며, 인쇄문서 및 PC나 정보저장매체 등에 의해 전자문서의 형태로 존재하는 것을 말한다.

② "정보시스템"이란 회사가 보유하고 있는 컴퓨터, 전산시스템, 네트워크, 소프트웨어 및 각종 영

상매체시 설물 등 "정보"를 관리하는데 필요한 모든 자산을 말한다.

제 6 조【보안대상 자산기준】

조직의 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.

1) 보안컨설턴트용 실무가이드북, 중소기업청, 2007 194 195 부록 영업 비밀 보호 서약서(예시) 중소기업기술 보호 지침

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 주어 진 사용자에게 정보 서비스를 거부하지 않아야 한다.

④ 준거성(Compliance) : 정보통신망 이용촉진 및 보안 등에 관한 법률, 부정경쟁방지 및 영업비밀 보호에 관한 법률 등 관련 법률의 요구사항을 준수하여야 한다.

제 7 조【보안기능】

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 부여 하고 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 발 생 시 책임을 추적할 수 있어야 한다.

⑤ 기타 : 정보자산에 대해 제6조(보안대상 자산기준)의 기준에 적합한 기능이 제공되고 관리되어야 한다.

제 8 조【보안조직】

회사는 정보자산의 보호와 관리를 위해 보안관리 부서를 별도로 마련하고, 회사 내 보안 관리 업무수행을 위하여 다음과 같은 조직을 구성한다.

① 보안책임자 : "일반보안업무"와 "IT보안업무"등 회사 내 보안관리 업무를 총괄·조정하고, 준수 여부를 감독한다.

② 보안관리자 : 보안 관리자는 보안책임자의 지시와 위임을 받아 보안관리 전반에 관한 업무를 수행하며, 보안관리자는 경영지원팀장이 겸한다.

③ 보안담당자 : 보안책임자가 관련 부서의 협조를 받아 분야별, 부서별 보안담당자를 선임한다.

④ 보안관리위원회 : 보안관리위원회는 회사 내 임원급 회의 구성원을 참석대상으로 하며, 보안책임자가 회의를 주재한다. 보안정책의 제·개정 및 주요 의사결정은 보안관리위원회에서 의결하며, 대표이사의 최종결재를 득한 후 시행한다.

제 3 장 정보자산의 분류

제 9 조【자산의 분류】

① 회사의 정보자산은 그 중요도에 따라 "극비", "대외비", "일반"등 3단계로 분류한다.

② "극비"란 주로 경쟁사 및 대외로 유출될 경우 기업 활동에 중대한 영향을 미쳐 회사가 막대한 손해를 입을 수 있는 정보를 말한다. 여기에는 회사 업무상중요하게 취급되는 인사, 급여 등의 정보를 포함한다.

③ "대외비"란 경쟁사 및 대외로 유출될 경우 회사에 피해를 줄 수 있는 정보 중 "극비"에 해당하지 않는 것을 말한다.

④ "일반"이란 "극비"또는 "대외비"가 아닌 그 이외의 정보를 말한다.

⑤ 자산의 분류는 일정 기간마다 새롭게 지정·변경 및 해제가 가능하다.

제 10 조【자산등급 결정】

각 정보자산의 등급은 정보의 생성시점에 소유자가 부여한다. 부여 시에는 정보를 적절하게 보호할 수 있도록 과대 또는 과소 분류되지 않도록 주의해야 한다.

제 4 장 인적보안

제 10 조【보안서약서 작성】

① 모든 임직원의 입·퇴사 시와 연봉계약시 보안서약서를 작성한다.

② 회사와 상호 협력관계를 유지하는 모든 국내외 업체 또는 개인은 매 계약체결시마다 보안서약서를 작성한다.

③ 보안책임자는 기타 특별관리가 필요한 업무 수행업체 또는 수행자에 대해 별도의 보안서약서를 징구하여야 한다.

제 11 조【보안교육】

① 모든 임직원은 입사지 사내 보안교육을 받도록 한다.

② 모든 임직원을 대상으로 년 1회 이상 보안교육을 실시한다.

③ 보안담당부서 소속 임직원은 반기 1회 이상 보안교육을 받도록 한다.

④ 보안교육은 외부 전문 업체에 위탁 실시할 수 있다

제 12 조【퇴직관리】

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

제5장 물리적 보안

제 13 조【시설관리】

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

제 14 조【장비관리】

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

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

② 장비의 반출 : 장비가 외부로 반출되거나 반입되는 경우 사전승인 절차를 반드시 거쳐야 하며, 그 사실을 관리대장에 기록하여야 한다.

제 15 조【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.

제 16 조【일반구역】

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

제6장 정보시스템 보안

제 17 조【정보시스템 운영】
정보자산의 비밀성, 무결성, 가용성 확보를 위해 보안책임자는 모든 정보시스템에 대한 운영 및 관리절차를 수립하고, 이에 따라 관리담당자를 지정하여 관리하도록 조치하여야 한다.

제 18 조【컴퓨터 사용】
회사 내 모든 컴퓨터 사용자는 불법소프트웨어를 사용해서는 안되며, 불법소프트웨어 사용으로 인한 모든 책임은 사용자에게 있다.

제 19 조【서버관리】
회사의 정보시스템을 구성하는 모든 서버들에 대해 적절한 보안관리 및 통제방안을 수립하여 관리하여야 한다.

제 20 조【네트워크 관리】
네트워크상의 정보 등을 보호하기 위하여 보안책임자는 별도의 담당자를 임명하고 적절한 보안관리 및 통제방안을 수립하여 관리하여야 한다.

제 21 조【접근통제】
보안관리자는 인가받은 사람만이 정보에 접근 할 수 있도록 접근통제 정책을 문서화하여 유지관리하여야 한다. 접근통제를 위해서는 적절한 권한의 부여 및 삭제, 사용자 패스워드 관리, 인가된 자에 대한 출입관리 등이 고려되어야 한다.

제7장 기타 보안관리

제 22조【보안준수】
모든 임직원, 협력업체 직원은 보안과 관련된 정책, 지침, 절차 등을 준수해야 한다.

제 23 조【보안점검】
① 회사는 년 1회 이상 정기적으로 임직원과 각 부서를 대상으로 보안점검을 실시하여야 하며, 필요시 특정 임직원 및 부서를 선정하여 불시에 점검할 수 있다.
② 보안점검 결과는 최고경영자에게 보고되고 회사 전체에 공지되어 자체적인 개선활동이 이루어지도록 조치한다.

제 24 조【보안계획 수립】

① 매년 보안계획을 수립하여 보안책임자의 승인을 얻은 후 시행한다.

② 보안계획을 수립하기 전에 회사의 보안요구사항을 파악하고, 내·외부의 보안위협 및 취약점에 대해 외부전문가를 활용하여 대응책수립을 위한 위험평가업무를 수행한다.

제 25 조【법규준수】

보안 업무를 수행함에 있어 국내 관련 법규를 준수하여야 한다

부 칙

제 1 조【시행일】

1. (2022년 12월 23일 개정) 이 규정은 2023년 01월 01일부터 시행한다.