정보보안 규정

제정 2024년 07월 19일

제1장 총 칙

제1조(목 적)

이 규정은 ㈜한빛레이저(이하 “회사”라 한다)의 보안업무 수행에 필요한 절차와 운용사항을 규정함을 목적으로 한다.

제2조(적용범위)

① 이 규정은 회사의 임직원(이하 “사원”이라 한다) 및 회사를 위해 종사하는 외부인 모두에게 적용된다.

② 회사가 보유하고 있는 지적재산권, 영업 비밀 등 기술상, 경영상의 내용 자체와 이를 포함하고 있는 문서, 정보시스템, 소프트웨어, 영상매체, 시설, 기타 유·무형의 모든 자산을 보호대상으로 한다.

제3조(보안조직)

회사는 보안업무를 효율적으로 수행하기 위해 보안조직을 구성할 수 있다. 보안책임자, 보안관리자, 부서별 보안담당자로 구성하고 역할과 책임을 명확히 한다.

제4조(보안조직의 역할과 책임)

보안조직의 역할과 책임은 다음 각 호와 같다.

1. 보안책임자는 사장으로 한다. 보안책임자는 보안관련 업무를 지휘, 감독한다.
2. 보안관리자는 보안관리부서의 부서장으로 한다. 주관부서가 없을 경우 사장이 임명한 자로 한다. 보안관리자는 보안업무를 총괄한다.
3. 부서별 보안담당자는 각 부서장으로 한다. 부서별 보안담당자는 각 부서의 보안책임자로서 자산에 대한 보안상태를 점검하여 적절한 조치를 취하여야 하며 소속사원들이 회사의 보안 규정을 준수하도록 교육하고 이행상태를 점검하여야 한다.

제2장 보안 준수사항

제5조(보안서약)

① 사원이 회사 재직 중 업무와 관련하여 합법적으로 생성하거나 획득한 모든 유·무형 자산에 대한 소유권 등 제반 권리는 회사에 있으며, 사원은 재직 중 또는 퇴사 후에도 회사의 승인 없이 이를 외부에 유출, 배포, 전송할 수 없다.

② 사원은 입사·퇴사 시 보안서약서의 내용을 숙지하고 서명 날인해야 하며, 보안서약서에는 다음과 같은 내용을 포함한다.

1. 회사 지적재산권 보호에 관한 준수

2. 영업비밀 및 고객정보 보호에 관한 준수

3. 회사 내에서 사용하는 개인 메일 및 메신저 감사 동의(사내 인트라넷 메일, 메신저 뿐 아니라

사내에서 회사 PC, 통신장치 등으로 주고받는 개인 메일 포함)

4. 제3자의 지적재산권 및 영업권 보호 준수

5. 기타 회사와 관련된 법규 및 요건에 관한 준수

③ 보안서약서 작성 시 자필로 작성하며 수정이 불가능한 볼펜 등의 필기구를 이용한다.

④ 사원은 회사에서 공지하는 보안규정 내용을 숙지하고 이에 따른 행동을 할 의무가 있다.

제6조(보안교육)

① 회사는 사원 및 협력회사의 사원 또는 필요 시 고객 및 방문객에게 회사의 보안규정 체계, 보안의 중요성 및 위반으로 인한 피해사례 등을 내용으로 하는 충분한 교육 훈련 및 관련자료를 제공한다.

② 전 사원은 년 1회 이상, 신규 입사자 및 진급자는 회사에서 요구하는 보안교육을 이수하여야 한다.

③ 퇴직 예정자는 퇴직자 보안준수사항에 대한 교육을 실시한다.

④ 보안책임자, 보안관리자 및 담당자 등 보안조직의 보안 전문성을 강화하기 위해 사내외 보안 전 가를 통한 교육을 실시한다.

제3장 전자문서 및 일반문서 보안

제7조(전자문서 및 일반문서 보안)

① 모든 문서는 관계사원만이 취급하는 것을 원칙으로 한다. 완결된 문서는 안전한 서류함(캐비닛, 파일박스 등)에 보관하고 퇴사 시에는 반드시 시건장치를 하여야 한다.

② 사원은 문서 등 정보자산의 생성 시 회사의 비밀분류기준에 따라 중요정보는 “극비”, “대외비”로 구분하며, 이외는 “일반”의 3 등급으로 구분 표시하여 관리하여야 한다.

1. 극비란 회사 내·외부에 공개되거나 누설될 경우, 회사의 조직 활동에 중대한 영향을 미칠 가능성이 있는 정보로서, “업무상 알 권한이 있는 한정된 사원”에게만 제공되도록 관리되어야 하는 정보이다.

2. 대외비란 업무상 회사 내부에서 취급되어야 하는 정보로서, 원칙적으로 회사 사원만 취급할 수 있고, 외부에 배포 시 문제를 야기하거나 손실을 가져와 반출을 억제해야 하는 정보이다. 대외비문서는 별표1과 같이 그 문서의 표면 중앙상단에 적색으로 표시하고 보호기간 및 보존기간을 기입하여야 한다.

3. 일반이란 회사의 이익을 위해 비용을 투입하여 구입했거나 제작한 자산으로 외부로 유출되더라도 해당 자산의 구입 및 제조 비용 이상의 손실은 없는 정보 자산, 또는 이미 외부에 널리 공개되었거나 회사의 사업과 무관한 정보를 담고 있는 정보 자산을 의미하며, 정보 자산 중 “극비”, “대외비” 정보 자산이 아닌 것을 말한다.

③ 사원은 “대외비” 이상의 생성·획득된 모든 전자문서를 회사가 지정하는 파일서버에 암호화하여 저장해야 하며, 사원 개인PC에 보관을 금한다. 일반보안문서의 경우 시건장치가 있는 보관장소에 별도 보관 관리하여 한다.

④ 비밀등급이 “대외비” 이상의 문서에 대해서는 비밀등급을 문서 표지에 표기하여 관리하여야 하며, 대외 유출이 필요한 경우에는 부서장 이상의 사전 승인을 득해야 한다.

⑤ 회사의 외부 유출을 목적으로 하는 모든 문서는 전자적으로 유통 시 임의 수정이 불가하도록 PDF, 이미지 파일로 변환하여 송부함을 원칙으로 하며, 제 3자가 편집하여 재활용 할 수 없도록 경고 문구를 삽입하여야 한다.

⑥ 사원은 회사 자산의 유출 위험성이 인식되면 지체없이 소속 부서장 또는 보안 담당자에게 신고하여야 한다.

제4장 출입통제 및 시설보안

제8조(출입통제 및 시설보안)

① 출입 통제 구역은 보안상의 중요도에 따라 “제한구역”, “보안구역”, “허가구역”으로 구분 관리하여야 한다.

1. 제한구역이란 보안구역 중 회사 내외부에 노출될 경우, 회사에 중대한 영향을 미칠 가능성이 있는 업무를 하는 구역으로, 업무상 출입권한이 있는 사원에게만 접근을 허용하는 구역이다. 연구소 및 개발관련 부서가 이에 해당된다.
2. 보안구역이란 업무상 “대외비” 이상의 정보가 노출될 수 있는 구역으로 외부인의 접근이 통제되며, 원칙적으로 회사의 사원만 출입할 수 있으며, 외부인은 부서장의 승인을 득한 경우에만 출입이 가능하다. 대부분의 사무공간이 이에 해당된다.
3. 허가구역이란 외부인의 접근이 허용된 구역으로 외부인과의 면담을 위한 접견실, 상담실 등이 이에 해당된다.

② 제한구역 또는 보안구역으로 설정된 곳은 출입자가 쉽게 볼 수 있도록 출입문 중앙 또는 잘 보이는 곳에 별표1과 같이 표시를 하여야 한다.

③ 사원은 사내에서 사원증을 상시 착용해야 하며 퇴사자는 사원증을 인사담당부서에 반납하여야 한다.

④ 사원증을 분실 또는 훼손하거나 기재사항의 변동으로 재발급받고자 하는 사원은 그 사유가 발생한 날로부터 5일 이내에 신분증 재발급신청서에 의해 소속부서장의 승인을 득한 후 인사담당부서에 제출하여야 한다. 인사담당부서는 신분증 발급대장에 등록하여 관련 사항을 관리하여야 한다.

⑤ 사원은 자신이 지급 받은 사원증을 어떠한 경우에라도 타인에게 대여하거나 양도할 수 없다.

제5장 PC 및 정보시스템 보안

제9조(PC 및 정보시스템 보안)

① 사원은 회사에서 승인된 하드웨어 및 소프트웨어 이외에는 사내에 설치하거나 사용할 수 없으며 필요 시 관련 부서장의 승인을 득한 후 보안관리부서의 보안성 검토 인가를 받아 사용해야 한다.

② 사원은 회사에서 지급한 PC로 업무를 수행하여야 하며, 개인 목적으로 등 PC의

저장장치 및 주요부품 등을 임의로 교체하거나 제거할 수 없으며, 허가되지 않은 통신장치나 보조 저장장치를 설치 할 수 없다.

③ 사원은 회사에서 지급한 업무용 PC 및 정보기기에 대해 다음과 같은 기준은 준수하여야 한다.

1. 회사에서 제공하는 바이러스 백신, PC보안프로그램, 윈도우OS 보안패치를 설치하고 항상 최신 버전을 유지한다.

2. 로그인, 화면보호기 패스워드를 설정하며, 파일공유는 원칙적으로 금하되, 필요 시, 회사 보안 정에 따르며 반드시 패스워드를 설정하여 공유한다.

3. 화면보호기 설정 시 대기시간은 10분 이내로 설정한다.

④ 사원은 노트북 PC를 사용하지 않을 때에는 잠금 장치를 이용하여 안전하게 보관하여야 한다.

⑤ 사원은 자신의 정보시스템 사용자 ID와 패스워드를 타인과 공유하여 사용하거나 누설해서는 안 되며 타인의 ID를 불법적으로 사용할 수 없다.

⑥ 사원에게 효율적인 업무 수행을 보장하기 위해 보안관리부서는 정보시스템 개발 및 운영 보안, 서버보안, 데이터베이스보안, 네트워크 보안 등의 상세 동제 대책을 수립하여 운영하여야 한다.

제10조(통신기기 보안)

① 사원은 전화, 프린터, 팩스 등의 통신기기를 통하여 회사의 전략 및 영업비밀 등 “대외비” 이상의 내용을 사외로 유출할 수 없다.

② 사원은 전화를 통한 회사의 중요 정보를 내용으로 하는 통화를 자재하여야 한다.

③ 사원은 회사에서 휴대폰 및 모바일 기기를 포함하여 승인하지 않은 유무선 송수신기기, 영상 촬영 및 플래시 메모리 등의 정보저장매체를 이용하여 비 인가된 회사 정보자산을 보관 및 전송할 수 없다.

제11조(네트워크, 인터넷 등 보안)

① 사원은 회사가 제공하는 장비와 할당된 IP만을 사용하여야 한다. 승인되지 않은 네트워크장비를 활용하여 회사의 정보통신망에 접근하는 행위를 금한다. 업무상 필요시에는 소속 부서장 및 보안관리 부서의 사전 승인을 득하여야 하며, 반드시 접근통제와 암호화 등의 조치 후 설치, 사용하여야 한다.

② 사원 또는 회사의 업무와 관련된 제3자는 회사에서 지정한 이메일·메신저시스템 이외의 외부 시스템을 이용하여 인가 없이 회사의 정보를 외부로 전송할 수 없다.

③ 사원은 웹하드, 블로그, P2P, 외부게시판, 포탈 커뮤니티, FTP 및 이와 유사한 인터넷 서비스를 이용하여 허가 없이 회사의 정보를 전송할 수 없다.

④ 사원은 회사의 정보통신망을 통해 대외로 유출되는 모든 이메일·메신저 또는 인터넷 서비스 내용에 대해 회사가 감사 및 모니터링 하는 것에 동의해야 한다. 이에 동의하지 않는 사원은 회사의 정보통신망을 통해 이메일·메신저 및 인터넷 서비스를 이용할 수 없다.

⑤ 사원은 회사가 제공하는 정보통신망을 이용하여 불건전 사이트 및 비업무용사이트 등의 접속을 제한한다. 업무상 필요시에는 소속 부서장 및 보안관리부서의 사전 승인을 득하여야 한다.

⑥ 사원의 회사 내의 정보통신망을 이용하여 다음 각 호와 같은 행위 및 이에 준하는 유사한 모든 행위는 금한다.

1. 회사가 보유한 지적재산권, 영업비밀 등의 정보자산의 비 인가된 유출 행위
2. 정당한 절차를 밟지 않고 타인 이메일 등을 개봉, 열람하는 행위
3. 회사가 제공하는 정보통신망 체계의 보안을 위협하는 행위
4. 이메일·메신저 등에 대한 회사의 정당한 접근과 열람을 방해하기 위해 암호 지정, 각종 소프트웨어 적용 행위
5. 회사에 손실을 초래할 수 있는 보안 위반 행위

⑦ 사원은 회사의 정보통신망을 통하여 불법적으로 제3자의 정보를 획득하려는 활동을 해서는 안 된다. 사원은 외부인과의 의사소통 시 이러한 점에 유의하여, 이메일, 메신저 등을 사용해야 한다.

⑧ 바이러스 확산 등 회사의 정보통신망 체계의 보안을 위협한다고 판단될 시에는 원인제공 컴퓨터에 대해 정보통신서비스 사용을 사전 통보 없이 일시적으로 제한할 수 있다.

⑨ 보안 관리자는 퇴사자가 자신의 계정으로 회사 이메일, 사내 인트라넷 등의 업무 시스템 및 회사 네트워크에 접속할 수 없도록 퇴사일 기준으로 즉시 조치해야 하며, 인사담당자는 퇴직예정자 정보를 퇴직일 1일 전까지 보안관리자에게 제공하여야 한다.

제6장 보안사고 및 징계

제12조(보안사고의 관리 및 통제)

① 보안사고란 고객정보 또는 회사 비밀정보의 유출, 변조 및 침해사고 등을 포함하며, 침해사고란 해킹 또는 컴퓨터바이러스 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.

② 보안관리부서는 보안침해사고 예방을 지속적으로 모니터링을 수행하고, 탐지된 불법 침해사고에 즉각 대응할 수 있도록 사고 대응 절차 및 체계를 구축하여 운영해야 한다.

제13조(보안규정 위반 시 징계)

① 사원 및 외부지원 인력의 보안규정 위반 사항 발생 시 보안관리부서는 보안책임임원에게 즉각 보고해야 하고, 사안의 경중에 따라 해당 사원의 인사위원회 회부 여부 및 법률적 위반사항에 대한 사항을 검토해야 한다.

② 보안사고 관련하여 인사위원회에 회부된 사원에 대해서는 내부의 징계기준을 의해 조치해야 하고, 외부인력의 경우 해당자 및 관련자에 대해서 엄중한 경고 또는 위중한 사안인 경우 계약 해지 조치, 관계기관 조치 의뢰 등 법률적 대응방안을 검토한다.

제7장 개인정보보호

제14조(개인정보보호 정책 수립 및 적용)

① 개인정보는 회사가 수집 또는 보유, 관리하는 개인에 관한 정보로서 성명, 주소 또는 주민등록번호 등 개인을 식별할 수 있는 정보를 말한다. 개인정보는 회사의 극비정보에 준하여 취급, 관리해야한다.

② 회사는 신용정보의 이용 및 보호에 관한 법률 등 관련 법령의 기준에 부합하도록

개인정보보호 정책 및 관리 기준을 수립하고 이를 시행하여야 한다.

③ 회사는 개인정보에 대한 접근기록을 보관하며, 비인가자의 접근여부를 관리한다.

④ 회사는 개인정보관리책임자, 개인정보관리담당자, 개인정보취급자를 대상으로 개인정보보호에 관한 교육계획을 수립하고 교육을 실시한다.

(별표1)

대외비문서 표시

대 외 비
2024. 01.

비고 : ① 가로 7cm x 세로 2cm

② 대외비문서는 위와 같이 그 문서의 표면 중앙상단에 적색으로 표시하고 보호기간 및 보존기간을 기입한다.