VALEX Service

제·개정 이력

일자	버전	내용	작성자
2024.07.01	1.0	신규 제정	김국기

정보보안규정

제 1 장 총칙

제1조(목적) 본 정보보안규정(이하 "규정")은 ㈜발렉스서비스(이하 "회사")의 정보보호를 위한 최상위 규정으로서, 회사의 정보자산을 안전하고 체계적으로 관리하기 위한 기본방침을 정립하여, 회사의 발전을 목적으로 한다.

제2조(적용범위) 본 규정은 회사에 소속된 임직원, 계열사 직원, 계약 관계에 있는 파트너사 직원, 회사를 방문하는 모든 외부인뿐만 아니라 회사가 소유, 보유하거나 회사에서 생성된 모든 유무형 자산에 대하여 적용하여야 한다.

제3조(역할과 책임) ① 임직원은 경영 목표를 달성하는데 있어서 정보보호를 반드시 고려해야 한다.
② 임직원은 규정 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 유지할 책임이 있다.
③ 정보보호 주관부서는 업무상 필요한 최소한의 사람만 정보에 접근할 수 있도록 관리해야 하며, 접근 승인을 받은 자는 해당 정보자산을 사용함과 동시에 보호할 책임을 갖는다.
④ 회사는 규정에 따른 임직원의 업무 활동에 필요한 적절한 대책과 교육을 수행해야 한다.

제 2 장 정보보호 규정 및 지침 운영

제4조(규정 및 지침 수립) ① 정보보호 규정 수립 시, 회사의 업무 특성 및 국내 유관법령, 규제 등을 반영하여 수립해야 한다.
② 규정의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 명시한 정보보호 지침을 수립할 수 있다.

제5조(승인 및 공표) ① 회사는 제·개정한 정보보안규정을 최고 경영진의 승인을 득한 후 공표하며, 공표한 날로부터 시행해야 한다.
② 정보보호 주관부서는 정보보호 규정 및 지침을 전 임직원이 상시 열람할 수 있도록 인쇄물 또는 전자문서 형태로 공표, 게시해야 한다.

제6조(유지 관리) 정보보호 주관부서는 정보보호 규정 및 지침의 타당성과 적합성을 주기적으로 검토하고, 그 결과를 반영해야 한다.

제 3 장 정보보호 조직

제7조(정보보호 조직체계) ① 회사는 정보보호와 관련하여 명확한 방향 제시, 임직원의 참여, 책임의 부여 및 주기적인 검토 등을 통하여 적극적인 지원을 제공해야 한다.
② 회사는 다음의 역할을 원활히 수행할 수 있도록 정보보호 지식과 경험을 갖춘 임직원을 지정하여야 한다.

1. 정보보호책임자
2. 정보보호관리자
3. 관리, 물리, 기술 영역 정보보호담당자

③ 회사는 정보보호책임자의 역할을 지원하고 정보보호 활동을 체계적으로 이행하기 위한 정보보호 조직을 구성하여 운영해야 한다.
④ 회사는 정보보호관리자를 지정하여 정보보호 관련 실무 활동을 체계적으로 이행하도록 한다.

제8조(정보보호 조직의 책임과 역할) 회사는 정보보호 조직의 각 구성원들의 역할과 책임을 구체화하여 정보보호 조직의 운영 및 관리를 원활히 할 수 있도록 한다.

제 4 장 인적 보안

제9조(비밀 유지) 인사·교육팀은 직원의 입사 시 정보보호 규정 및 지침을 이해하고 이를 준수하겠다는 내용의 보안서약서를 징구해야 한다.

제10조(퇴직 및 계약 해지) ① 임직원은 퇴사 및 계약 해지 시 회사 소유의 모든 정보자산을 반납하고, 근무 기간 중 습득한 정보에 대한 비밀을 준수할 것을 서약하는 비밀유지 서약서를 제출해야 한다.
② 정보보호 주관부서 및 관련 부서는 직원의 퇴사, 계약 해지 시 회사 소유의 정보자산 및 접근 권한을 즉시 회수해야 한다.

제11조(인사 이동 시) ① 정보보호 주관부서는 임직원의 인사이동 및 직무변경 시 기 부여한 접근 권한의 적정성을 확인하여, 불필요한 권한을 즉시 회수해야 한다.
② 정보보호담당자는 인사이동 및 직무변경 시 부서 내 공용으로 사용하는 계정의 권한을 즉시 변경해야 한다.

제12조(정보보호 교육) ① 정보보호책임자는 연간 정보보호 교육 및 훈련 계획을 수립해야 한다.
② 정보보호 교육 및 훈련은 전 임직원을 대상으로 정기적으로 실시해야 한다.
③ 정보보호 교육은 직무 및 전문성을 고려하여 교육 대상에 따라 차별화해야 한다.

제13조(정보보호 상벌 제도) ① 임직원의 정보보호 인식 제고 및 규정의 준수를 위하여 상벌 제도를 운영할 수 있다.

② 포상 및 징계 수준은 사건의 경중을 고려하여 유관부서와 협의를 통하여 결정해야 한다.

제 5 장 정보자산 관리

제14조(정보자산의 책임과 권한) 회사는 소유하고 있는 정보 및 정보시스템 등 정보자산을 식별하고 통제, 관리, 감독해야 한다.

제15조(정보자산의 분류) ① 정보자산은 회사가 소유, 보유하거나 회사로부터 생성된 출력문서, 전자문서 등을 포함한 모든 유무형의 정보 및 기술, 자료, 시설 등을 포함한다.
② 정보자산은 유형에 따라 다음 각 호와 같이 분류하여 관리해야 한다.

1. 전자정보 : 데이터베이스, 데이터 파일 등 전자적 형태로 저장되는 정보를 말한다.
2. 문서정보 : 출력 또는 수기로 작성한 문서 형태의 자료(계약서, 제안서 및 수행 산출물 등)를 말한다.
3. 정보시스템 자산 : 전자정보 및 문서정보의 전자적 업무 활용을 위한 서버, 네트워크, 보안시스템, 어플리케이션 등을 말한다.
4. 시설·설비 자산 : 전력, 항온·항습, 소화설비 등의 시설 인프라 및 물리적 출입 통제장치, 영상처리기기 등 설비를 포함한다.

제16조(정보자산의 파기) ① 관리적 정보보호담당자는 정보자산의 보존이 불필요할 경우 지체 없이 파기해야 한다.
② 정보자산은 복구 또는 재생할 수 없는 방법을 이용하여 파기해야 한다.
③ 정보자산의 파기를 파트너사에 위탁하는 경우, 관리·감독 등 보호 조치를 취해야 한다.

제 6 장 접근통제

제17조(사용자 접근통제) ① 기술적 정보보호담당자는 사용자 및 업무의 중요도, 접근 과정에 따른 위험 등을 고려하여 1개 이상의 인증 방식을 시스템에 적용해야 한다.
② 기술적·관리적 정보보호담당자는 중요정보 또는 외부 인터넷 망을 통해 내부시스템, 관리자 페이지, 중요정보에 접근하는 경우, 추가적인 인증 또는 안전한 접근 수단을 사용하도록 해야 한다.

제18조(계정 관리) ① 계정의 신규 등록, 삭제 또는 변경 사유가 발생한 경우, 관리적 정보보호담당자에게 요청하여 처리 해야 한다.
② 모든 계정은 사용자 별로 개별 부여해야 한다.
③ 시스템 특성 상 공용 계정 사용이 불가피한 경우, 정보보호 주관부서의 승인을 득해야 한다.
④ 임시 계정 발급 시 계정의 유효기간을 설정하여 유효기간이 지나면 사용정지 되도록 설정해야 한다.
⑤ 관리적 정보보호담당자는 정기적으로 계정 현황을 확인하여, 불필요한 계정을 삭제 또는 비활성화 해야

한다.

제19조(비밀번호 관리) ① 정보시스템 접속 비밀번호는 안전한 비밀번호를 생성, 관리해야 한다.
② 타인과 비밀번호를 공유하는 행위를 금지한다.
③ 비밀번호는 사용자가 직접 주기적으로 변경해야 한다.
④ 정보보호책임자는 비밀번호 입력, 변경, 저장 및 전송 시 노출되지 않도록 시스템을 구현해야 한다.

제20조(권한 관리) ① 업무 목적상 필요한 최소한의 권한만 부여해야 한다.
② 권한 부여, 변경, 삭제 등 변경 사유 발생 시 사전에 승인을 득해야 한다.
③ 권한 부여, 변경, 삭제 등의 이력을 기록, 보관해야 한다.
④ 관리적 정보보호담당자는 부여한 권한의 적정성을 정기적으로 검토 및 평가를 시행, 조정해야 한다.

제21조(정보시스템 접근통제) 기술적 정보보호관리자는 다음 각 호를 고려하여 시스템을 구현·운영해야 한다.

1. 접속 실패 시 최소한의 정보만 표기하고, 관련 기록을 남기도록 시스템을 설정해야 한다.
2. 접속오류 횟수가 비정상적일 경우에는 접속을 차단하고 해당 계정을 일시적으로 사용 중지하도록 설정해야 한다.
3. 접속 후 일정 시간 동안 사용하지 않는 경우, 자동 로그오프 또는 세션을 종료하도록 설정해야 한다.
4. 하나의 계정으로 여러 단말기에서의 동시접속을 제한해야 한다.

제22조(네트워크 접근통제) ① 정보보호 주관부서는 필요한 최소한의 범위 내에서 접근을 허용해야 하며, 변경 내역을 기록·관리해야 한다.
② 내부 네트워크와 외부 네트워크의 연결(대외 기관, 외부 통신망, 인터넷 등) 또는 변경시에는 필요한 보호대책을 수립하여, 정보보호 주관부서의 승인을 득해야 한다.
③ 정보보호 주관부서는 정보보호 관련 법규를 고려하여 필요 시 사용자 단말, 정보시스템등을 대상으로 인터넷망과 업무망을 분리해야 한다.

제23조(인터넷 접근통제) ① 정보보호 주관부서는 비 업무용 사이트 및 불법 파일 전송이 가능한 사이트의 접속을 제한해야 한다.
② 정보보호 주관부서는 인터넷을 통한 악성코드의 사내 유입 및 확산을 탐지·모니터링 해야 한다.

제24조(무선 접근통제) ① 무선 네트워크 접속은 회사에서 인가한 무선접속장비를 이용한 접속만 허용한다.
② 관리적 정보보안담당자는 비인가 무선접속장비가 사내망에 식별되는 경우 즉시 차단한다.
③ 정보보호 주관부서는 비인가 무선접속장비의 설치·운용 여부를 보안점검 시 확인해야 한다.

제25조(원격 업무 접근통제) 정보보호 주관부서는 재택·파견·이동근무 등 원격 업무 시 정보자산 유출 등의

보안사고 방지를 위해 원격 단말기, 내·외부 네트워크, 원격 접속 수단 등에 대한 보호 대책을 강구하여야 한다.

제 7 장 물리 보안

제26조(보호구역의 설정) 물리적 정보보호 담당자는 회사의 관리하에 있는 물리적인 공간 중 보호해야 할 필요가 있는 구역을 보호구역으로 지정하고, 관리해야 한다.

제27조(보호구역의 접근통제) ① 물리적 정보보호 담당자는 보호구역에 대한 출입통제를 위해 별도의 출입통제장치 및 감시시스템 등을 설치·운영해야 한다.
② 외부인이 보호구역에 출입할 때에는 항상 인가된 출입증을 패용하고 임직원이 동행해야 한다.
③ 물리적 정보보호 담당자는 통제구역의 출입 이력을 확인할 수 있는 수단을 마련해야 하며, 주기적으로 출입 내역을 검토해야 한다.
④ 노트북, 이동식 저장 매체 등을 소지하고 통제구역에 출입할 때에는, 사전에 승인을 득해야 하며, 사전 승인된 물품 이외에는 반출·입 할 수 없다.
⑤ 임직원 퇴사 시 출입증은 즉시 반납하여야 하며, 반납된 출입증은 폐기 및 관리하여야한다.
⑥ 출입증 분실 시, 물리적 정보보호담당자에게 신속히 알려야 한다.

제28조(정보자산 반출·입) ① 정보자산을 반출·입 할 때에는 해당 부서장의 승인을 득해야 하며, 개인적 용도로 회사 정보자산을 반출하는 것을 금지한다.
② 정보자산의 반출 이력을 기록, 관리해야 한다.

제29조(전산 시설 보호 대책) 물리적 정보보호 담당자는 환경적 위해 요소 및 불필요한 접근 등으로부터 전산 시설을 보호하기 위한 관련 전산 설비 구축 등의 보호대책을 이행해야 한다.

제30조(사무실 보호대책) ① 물리적 정보보호 담당자는 문서 파기 장치를 임직원이 적절히 사용할 수 있도록 설치, 운영해야 한다.
② 중요 정보는 반드시 잠금 장치가 설치된 장소에 보관해야 한다.
③ 노트북은 반드시 잠금 장치를 통해 보호해야 하며 도난, 분실에 유의해야 한다.
④ 프린터, 팩스, 복사기 사용 시 산출되는 문서는 즉시 회수해야 한다.
⑤ 공용 PC 사용을 금지한다. 단, 사용이 필요한 경우 공용 PC 의 관리자를 지정하여 방치되거나 부당한 목적으로 사용되지 않도록 해야 한다.
⑥ 공용 캐비닛에는 관리자를 지정하고, 퇴실 시 항상 잠그며 열쇠는 안전한 곳에 보관해야 한다.

제 8 장 운영 보안

제31조(권한 분리) 권한 오남용을 예방하기 위해 정보시스템 운영 담당자, 개발자 직무 분리 및 직무 구분에 따른 권한을 분리 운영해야 한다.

제32조(정보보호 시스템 운영) 정보보호 시스템 운영자는 최신 정책 업데이트 및 이벤트 모니터링을 시행해야 하며, 정책의 등록·변경·삭제 시 정보보호 주관부서의 승인을 받아야 한다.

제33조(장애 관리) ① 정보시스템 운영자는 정보시스템을 지속적으로 모니터링 해야 하며, 이상 징후가 감지 될 경우 장애 여부를 판단하여 사안에 따라 대응해야 한다.
② 정보시스템 운영자는 장애 이력을 기록·관리해야 한다.

제34조(취약점 점검) ① 정보시스템 관리자는 주기적으로 시스템 취약점 점검을 수행해야 한다.
② 취약점 점검 결과 도출된 문제점에 대해 반드시 보호 조치를 적용해야 하며, 그 결과에 대해 이행 점검을 시행해야 한다.
③ 정보보호관리자는 취약점 점검 결과 및 개선조치 사항에 대하여 정보보호책임자에게 보고해야 한다.

제35조(공개서버 보안) ① 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치해야 한다.
② 공개서버의 관리자는 정기적으로 게시 정보의 적정성을 검토하여 개인정보 등 주요 정보가 노출되지 않도록 관리해야 한다.

제36조(정보시스템 저장매체 관리) ① 정보시스템 폐기 또는 재사용 시 해당 시스템에 저장된 정보는 복구할 수 없는 방법으로 삭제해야 한다.
② 정보시스템의 외부 수리 등 파트너사를 통해 업무를 처리하는 경우, 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치 하여야 한다.

제37조(악성코드 통제) ① 정보시스템 운영자는 서비스의 중요도, 데이터의 안전성 등 보안을 고려하여 시스템에 백신 프로그램을 설치해야 한다.
② 백신 프로그램은 항상 최신의 정보를 유지할 수 있도록 정기적으로 업데이트를 수행해야 한다.

제38조(패치 관리) ① 정보시스템 운영자는 정기적으로 패치 업데이트를 수행해야 하며, 적용 내역을 기록·관리해야 한다.
② 정보시스템 운영자는 패치 적용 전 안정성 테스트를 수행해야 한다.
③ 서비스 문제 등으로 인해 보안 패치를 적용하지 못하는 경우, 그에 따른 대응 방안을 마련해야 한다.

제39조(로그관리 및 모니터링) ① 정보시스템 관리자는 정보보호 사고 발생 시 추적이 가능하도록 시스템 접근 및 사용내역을 기록, 보관해야 한다.

② 로그 기록은 별도 저장매체에 백업해야 하며, 접근권한을 최소화해야 한다.
③ 모든 시스템은 로그에 대한 정확한 기록을 보증하기 위해 시간을 동기화해야 한다.
④ 정보시스템 관리자는 로그 기록을 정기적으로 검토해야 한다.
⑤ 주요 정보시스템은 침해 시도를 인지할 수 있도록 모니터링을 시행해야 하며, 이상 징후 발견 시 지체 없이 정보보호 주관부서에 보고해야 한다.

제 9 장 사용자 보안 관리

제40조 (PC 보안) ① 임직원은 PC 에 회사에서 운영하고 있는 보안 솔루션을 설치해야 하며 임의로 삭제할 수 없다.
② 사용자 임의로 하드웨어를 추가, 변경, 제거할 수 없다.
③ 임직원은 PC 에 그룹 화면보호기를 설정하고 대기시간을 10 분 이내로 하여 비밀번호를 설정해야 한다.
④ 업무 목적상 반드시 공유 폴더가 필요한 경우에는 접근 가능한 사용자 제한 등 보호대책을 수립·적용해야 한다.
⑤ 업무 목적상 휴대용 저장 장치 등의 매체 사용이 필요한 경우 정보보호 주관부서의 승인을 득해야 한다.
⑥ 임직원은 PC 에 설치한 운영체제, 어플리케이션 등의 최신 보안패치를 유지해야 한다.
⑦ 임직원은 본인이 지급받은 PC 에 대한 보안 및 관리에 책임을 다해야 한다.

제41조(악성코드 예방) ① 임직원은 단말기 보호를 위해 악성코드 탐지 및 대응 솔루션을 설치해야 하며, 정기적으로 업데이트 및 실시간검사를 수행해야 한다.
② 특별한 이유 없이 시스템 혹은 프로그램이 동작하지 않는 등 악성코드 감염이 의심되는 경우 정보보호 주관부서에 신고해야 한다.
③ 전자우편, 메신저, SMS 등을 통해 출처가 불분명한 상대에게 의심스러운 메일, 링크, 첨부파일을 수신한 경우, 임직원은 수신한 자료를 클릭하지 않고 정보보호 주관부서에 신고해야 한다.

제42조(불법 소프트웨어 사용 금지) 임직원은 회사에서 허가한 소프트웨어만을 사용해야 한다.

제 10 장 업무용 정보통신 수단의 이용 및 관리

제43조(업무용 정보통신 수단) ① 정보보호 주관부서는 사용자의 송·수신 기록을 확보할 수 있는 전자우편, 메신저 등을 임직원 업무용 정보통신 수단으로 지정해야 한다.
② 정보보호 주관부서는 업무용 정보통신 수단 외의 전자 우편, 메신저 등의 사용을 제한해야 한다.
③ 임직원은 업무용 정보통신 수단 외의 전자우편, 메신저를 사용해서는 안 된다.
④ 전자우편 및 메신저를 통해 중요 정보를 전송하는 경우, 암호화 등 보호 조치를 적용해야 한다.

제44조(업무용 정보통신 수단 로그 기록 및 관리) ① 전자우편, 메신저 시스템 관리자는 정보통신수단의 사용기록 및 송·수신 정보를 기록, 보관해야 한다.
② 정보보호 주관부서는 업무용 정보통신 수단의 로그 보관 상태를 주기적으로 점검해야 하며, 점검 결과를 기록, 관리해야 한다.

제 11 장 정보시스템 도입, 개발 및 유지보수

제45조 (정보시스템 개발과 운영 환경의 분리) ① 개발 및 테스트 시스템은 운영 시스템과 분리하여 설치, 운영해야 한다.
② 컴파일러, 편집기 등과 같이 개발에 필요한 도구를 운영환경에 설치하는 것을 금지한다.

제46조(요구사항의 정의) 정보시스템 도입, 개발 및 유지보수 담당부서는 정보시스템 도입, 개발 및 유지보수 시 다음 각 호의 보안 요구사항을 명확히 정의하여 관리해야 한다.

1. 사용자 인증 방법
2. 접근통제 방법
3. 입력 데이터 검증, 내부처리, 출력 데이터 검증
4. 로그 관리
5. 암호화
6. 개인정보의 화면 출력 시 마스킹 표시
7. 기타 개발·운영 시 정보보호 통제

제47조 (개발 시 보안) ① 개발자는 어플리케이션 개발 및 유지보수 시 보안 요구사항을 고려하여 어플리케이션을 개발해야 한다.
② 소스코드 내에 비밀번호 및 중요 개인정보의 기록을 금지한다.
③ 소스코드에 대한 변경이력을 관리해야 한다.
④ 신규 프로그램 구축을 위해서 사업 준비 단계에서부터 보안 요소를 반영한 소스코드 점검을 개발일정에 반드시 포함해야 한다.

제48조(소스코드 접근통제) ① 소스코드를 운영환경에 보관하는 것을 금지한다.
② 인가자만 소스코드에 접근할 수 있도록 보호 대책을 수립·적용해야 한다.

제49조(테스트) ① 개발자는 어플리케이션 신규 개발 및 변경 시 테스트 환경에서 해당 어플리케이션을 충분히 테스트하고 그 결과를 문서화해야 한다.
② 운영 환경의 실 데이터를 변경 없이 테스트 데이터로 활용하는 것을 금지한다. 단, 반드시 실 데이터를 사용해야 할 경우에는 비 식별 처리하거나 부서장의 승인을 받고 사용해야 한다.

③ 테스트용 데이터는 적절하게 관리해야 하며, 사용 이후 삭제 및 이력을 관리해야 한다.

제50조(정보시스템 도입 및 구축) ① 정보시스템 도입 및 구축 주관 부서는 정보시스템 신규 도입, 구축 시 보안 요구사항을 고려해야 한다.
② 신규 도입 및 구축한 정보시스템을 대상으로 취약점 점검 및 모의해킹을 수행해야 하며, 도출된 문제점에 대해 반드시 보호 조치를 적용해야 한다.

제51조(사전 보안성 검토) ① 신규 도입, 구축 및 개발한 정보시스템을 운영단계로 이관하기 전에 정보보호 관리자로부터 사전 보안성 검토를 받아야 한다.
② 정보보호 주관부서는 신규 정보시스템에 대한 보안성 검토를 실시하고, 그 결과를 문서화하여 관리해야 한다.
③ 신규 도입, 구축 및 개발한 정보시스템으로 인해 회사의 정보보호 수준이 저하될 경우, 정보보호관리자는 서비스 시작을 제한할 수 있다.

제 12 장 파트너사 관리

제52조(사업 준비단계 보안) 파트너사와 사업을 계약할 경우 다음 각 호의 내용을 반영해야 한다.

1. 사업 계약 시, 보안준수 사항 및 손해배상 책임 등을 문서화해야 한다.
2. 수탁 업체가 사업의 일부 또는 전부에 대하여 재 위탁 계약을 체결하는 경우, 반드시 회사의 동의 하에 진행되어야 하며, 본 계약 수준의 보안 준수 사항을 포함해야 하고 위반 시 손해배상 책임 등을 문서화해야 한다.
3. 기타 법령에서 요구하는 보안조치 사항

제53조(사업 수행단계 보안) ① 사업 주관 부서는 사업 참여 인력에 대하여 외부 인력용 보안서약서를 징구해야 한다.
② 외부 인력의 PC 를 회사 내부 네트워크에 연결하는 경우 임직원과 동일한 보안 정책을 적용해야 한다.
③ 사업 주관 부서는 파트너사에게 업무상 필요한 최소한의 정보 및 권한을 제공해야 한다.
④ 사업 주관 부서는 파트너사에게 제공한 정보 또는 수행 중 생성된 산출물에 대하여 인터넷, 웹하드 등의 자료 공유사이트에 업로드를 금지하고, 전자우편으로 수·발신하는 것을 금지해야 한다.

제54조(사업 종료단계 보안) ① 사업 주관 부서는 사업의 최종 산출물 중 보안이 요구되는 자료를 기밀 또는 대외비로 등록하여 관리해야 한다.
② 사업 주관 부서는 사업 완료 시 다음 각 호의 항목을 수행해야 한다.

1. 파트너사에게 부여한 물리적, 논리적 접근권한 및 정보자산을 회수해야 한다.
2. 외부 인력의 PC, 노트북 및 기타 저장장치내의 모든 자료를 복구가 불가능한 방법으로 삭제해야 한다.
3. 사업 수행 중 획득한 정보에 대한 비밀 유지 의무를 설명해야 한다.

제 13 장 침해사고 및 연속성 관리

제55조(침해사고의 정의) 회사는 다음의 내용을 해당하는 경우 침해사고로 분류하여 관리해야 한다.

1. 회사의 기밀정보 또는 개인정보가 유·노출되거나 위·변조된 경우
2. 주요 정보자산(H/W, S/W, DB 등)이 유출, 절도, 파괴된 경우
3. 악성코드 등에 의해 회사 서비스가 지연 및 중단된 경우(웹해킹, DDoS 공격 등)
4. 비 인가자가 회사의 정보시스템을 공격하거나 침투한 경우
5. 내부자 및 접근이 허용된 외부자에 의한 내부 자원의 오용
6. 물리적인 통제구역 또는 내부 전산망의 무단 침입

제56조(침해사고 대응체계 구축) ① 침해사고 대응을 위해 정보보호 최고책임자를 중심으로 침해사고 대응조직을 구성하고, 대응체계를 수립 운영해야 한다.

② 정보보호 주관부서는 정보자산에 영향을 미치는 침해사고의 심각한 정도를 정의해야 한다.

③ 침해사고 여부 등 이상징후를 파악하기 위해 모니터링 및 정기적인 로그 분석을 수행해야 한다.

제57조(침해사고 예방) 정보보호관리자는 침해사고의 효율적인 예방을 위해 다음 각 호의 사항을 포함한 침해사고 예방 활동을 시행해야 한다.

1. 정보보호시스템 운영
2. 접근통제 실시
3. 정기적 취약점 평가 실시
4. 규칙적인 백업 수행 및 소산 관리
5. 주요 정보시스템 이중화
6. 침해사고 대응 조직 구성 및 관련 비상 연락망 구축

제58조(침해사고 보고) ① 임직원 및 정보시스템 운영자는 침해사고가 발생하거나 징후를 포착하면 즉시 정보보호 주관부서에 신고해야 한다.

② 정보보호 주관부서는 침해사고 발생 또는 징후를 접수하였을 경우 해당 내용을 기록 및 관리해야 한다.

③ 정보보호 주관부서는 사고의 처리가 완료되면 침해사고에 대한 보고서를 작성해야 한다.

제 14 장 개인정보보호

제59조 (개인정보 내부관리계획 수립·시행) ① 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 개인정보 내부관리계획을 수립·시행해야 한다.

1. 개인정보보호책임자의 자격요건 및 지정에 관한 사항

2. 개인정보보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보내부관리지침의 수립 및 승인에 관한 사항
4. 개인정보의 기술적·관리적 보호조치 이행 여부의 내부점검에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 개인정보취급자에 대한 교육에 관한 사항
7. 접근 권한의 관리에 관한 사항
8. 접근 통제에 관한 사항
9. 개인정보의 암호화 조치에 관한 사항
10. 접속기록 보관 및 점검에 관한 사항
11. 악성프로그램 등 방지에 관한 사항
12. 물리적 안전조치에 관한 사항
13. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
14. 개인정보 유출사고 대응 계획 수립 및 시행에 관한 사항
15. 위험도 분석 및 대응방안 마련에 관한 사항
16. 그 밖에 개인정보보호를 위해 필요한 사항

② 제 1 항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 개인정보 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리해야 한다.

제60조(개인정보 위탁 관리) ① 개인정보 처리를 위탁하는 경우, 해당 위탁 업무의 내용과 수탁자에 대한 내용을 정보주체에게 공개해야 한다.

② 파트너사와 개인정보 관련하여 업무를 수행할 경우 개인정보 보호와 관련하여 다음 각 호의 요건을 계약서, 약정서 등에 문서화해야 한다.

1. 위탁업무 수행 목적, 범위 및 목적 외 개인정보 처리 금지에 관한 사항
2. 개인정보에 대한 비밀 유지 및 기술적, 관리적 보호 의무 준수
3. 개인정보보호 관리 부실로 인한 문제발생 시 손해배상책임
4. 개인정보 취급 활동에 대한 모니터링 및 감사 권한
5. 재위탁 제한에 관한 사항
6. 기타 개인정보의 안전한 처리를 위한 사항 및 법적 준수 사항

제61조(가명정보의 처리) 회사는 개인정보를 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 가명처리하여 활용할 경우 기술적·관리적·물리적 안전조치를 이행하고, 재 식별되지 않도록 관리하여야 한다.

제 15 장 규정 준수

제62조(규정 준수의 책임과 권한) 회사의 임직원은 정보자산 및 중요정보의 안전성을 확보하기 위해 본 규정 및 지침을 숙지하고 준수할 책임이 있다.

제63조(법률과의 관계) ① 본 규정은 업무를 수행함에 있어 안전성 확보를 위해 적용해야 할 기본적인 사항을 규정하는데 목적이 있다.

② 정보보호 관련 법령에 관해서는 본 규정에 앞서 우선 적용됨을 원칙으로 한다. 다만 관련 법령에서 규정하지 않는 조치사항에 대해서는 본 규정을 적용한다.

[별표 1]

보안서약서

소 속 :
직 위 :
성 명 :
생년월일 :

상기 본인은 ㈜발렉스서비스(이하 "회사"라 한다.)에 근무하는 기간은 물론 퇴사 후에도 회사의 영업비밀을 외부(제3자)에 일체 유출시키지 않을 것이며, 다음의 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 회사의,
   가. 진행중인 사업 및 영업현황과 일체의 사업 및 영업계획 등에 관한 사항
   나. 인사, 조직, 재무회계, 자금상황 등에 관한 사항
   다. 연구, 개발 등에 관한 사항
   라. 고객정보 및 타사와의 업무제휴 등에 관한 사항
   마. 기타 사업수행 시 중요하다고 판단되는 사항
   등을 회사의 영업비밀로 인지하고 회사의 보안관리 업무지침을 성실히 이행하겠습니다.
2. 본인은 본인이 알고 있는 알고 있는 제 3 자의 비밀을 여하한 일이 있어도 비밀보유자의 승낙 없이 회사에 공개하거나 업무에 부정하게 사용하지 않겠습니다.
3. 본인은 업무 중 지득한 회사의 영업비밀을 회사의 사전 승인없이 본인의 이익을 위하여 사용하지 않겠습니다.
4. 본인은 업무 중 지득한 회사의 영업비밀을 회사의 사전 승인없이 제3자 또는 경쟁업체를 포함한 동종업체에 누설, 유출 또는 제공하지 않겠습니다.
5. 본인은 회사를 퇴직한 후에도 회사 재직 시 지득한 영업비밀을 가지고 창업을 하거나 경쟁회사를 위하여 사용 하지 않겠습니다.
6. 본인은 회사를 퇴직한 후에도 회사의 영업비밀을 제3자 또는 경쟁업체를 포함한 동종업체에 누설, 유출 또는 제공하지 않겠습니다.
7. 만일 본인이 이 서약서의 내용 및 부정경쟁방지법의 관련 규정을 위반하여 회사에 손해가 발생한 경우 회사의 청구에 따라 그 손해를 배상할 것과 제반 민.형사상의 책임을 질 것을 서약합니다.

202 년 월 일

서 약 자: (인)

㈜발렉스서비스 대표이사 귀하

[별표 2]

비밀유지 서약서(퇴사)

소 속 :
직 위 :
성 명 :
생년월일 :

본인은 ㈜발렉스서비스(이하 '회사'라 함)를 퇴직함에 있어 아래 사항을 충분히 숙지하고, 성실히 준수할 것을 서약합니다.

1. 회사에 재직한 기간 중 독자적으로 또는 다른 사람과 함께 취득한 기술정보(발명, 특허, 개발, 생산 등 제반 기술) 및 경영정보(재무, 관리, 기획, 영업, 인사 등 제반 정보)등 모든 영업비밀은 전적으로 회사의 소유이며, 회사가 사용하거나 처분할 권리가 있음을 인정합니다.
2. 어떠한 장소에 어떠한 방법으로도 회사의 영업비밀 및 자산을 보유하거나 저장하고 있지 않음을 확인합니다.
3. 재직기간 중 취득한 회사의 모든 영업비밀(경영 및 기술정보)은 퇴사 후에도 회사의 업무 인수.인계와 관련 없는 어떠한 회사내외 제3자에게도 누설하지 않겠습니다.
4. 퇴직 후 3년간 회사의 영업 비밀을 이용하여 창업하거나 경쟁관계에 있는 회사 기타 제3자를 위하여 영업비밀을 누설하거나 사용하지 않겠습니다.
5. 회사의 영업비밀 보호를 위한 노력에 적극 협조할 뿐 아니라, 그에 따른 법적.도덕적 의무를 성실히 이행하겠습니다.

본인은 위의 사항을 충분히 숙지하여 이를 성실히 준수할 것이며 만일 이를 위반하였을 경우 부정경쟁방지 및 영업비밀에 관한 법률 등 관련 법령에 따라 민,형사상의 책임 뿐만 아니라 제반 손해 배상의 책임 등 불이익을 감수할 것이며, 회사에 끼친 손해에 대해 지체없이 변상.복구할 것을 서약합니다.

202 년 월 일

서 약 자: (인)

㈜발렉스서비스 대표이사 귀하

[별표 3]

보안서약서

소 속 :
직 위 :
성 명 :
생년월일 :

본인은 ㈜발렉스서비스(이하 '회사'라 함)에 OOO사업을 진행함에 있어, 다음 사항을 준수할 것을 서약합니다.

1. 회사의 보안구역 및 통제구역에 무단으로 출입하지 않는다.
2. 회사의 자산을 불법으로 유출, 변조하거나 훼손하지 않는다.
3. 회사의 자산을 개인적인 목적이나 이익을 위하여 사용하지 않으며, 허가된 용도로만 사용한다.
4. 허용되지 않은 정보자산에 접근을 시도하거나,정보보호 기능을 우회하는 시도를 하지 않는다.
5. 업무상 취득한 회사 또는 제3자 소유의 정보를 회사의 승인없이 누설하지 않는다.
6. 회사의 통신망을 이용하여 외부인 접근이 금지된 타 회사나 기관의 통신망 또는 시스템에 임의로 접속을 시도하지 않는다.
7. 회사의 자산(정보 포함)을 사용 후에는 즉시 회사에 전부 반환한다.
8. 기타 회사의 정보보호관련 규정을 준수한다.

본인은 위의 사항을 숙지하여 이를 성실히 준수할 것이며 만일 이를 위반하였을 경우 보안관계 제법 규정에 의거 처벌받음을 물론 어떠한 제재조치를 취하여도 이의를 제기하지 않을 것을 서약한다.

202 년 월 일

서 약 자: (인)

㈜발렉스서비스 대표이사 귀하

부 칙

제 1 조 (시행일)

개정된 정보보안규정은 2024년 08월 01일부터 시행한다.