작성	검토	승인

개인정보 보호 규정

기업명	동우ＨＳＴ 주식회사
문서번호	2022-G-3
제・개정일	2022.08.01
담당부서	윤리준법실
담당자	장수원 전무 / 조영지 실장

<제·개정 이력>

제·개정 번호	제·개정일	제·개정 사유
1	2022.08.01	최초 제정

동우HST㈜	개인정보 보호 규정	제・개정일
		2022.08.01

제 1 장 총 칙

제1조(목적) 이 지침은 다음 각 호의 보안 관련 상위 법규를 준수하고, 회사의 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 IT담당본부를 말한다.
3. "개인정보관리부서"라 함은 회사 고객의 개인정보보호 실무를 수행하는 개인정보보호조직으로서 개인정보를 취급하는 각 사업본부 및 정보보호담당부서를 말한다.
4. "시스템관리자"라 함은 각 정보시스템의 운영 및 관리를 담당하는 관리자 및 담당자를 말한다.
5. "정보보호 사고"라 함은 보호관리 대상에 속하는 정보 및 정보시스템이 무단으로 파괴되거나, 유출·변조되어 업무수행에 지장을 초래하는 사고를 말한다.
6. "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.
7. "정보자산"이라 함은 회사가 보유하고 있는 지적재산권과 영업비밀 등 기술상경영상의 내용 그 자체와 이를 포함하고 있는 문서, 네트워크, 서버, 정보보호시스템,응용프로그램, PC, 소프트웨어, 부대설비 및 기타 유무형의 모든 자산을 의미한다.

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

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

제4조(책임사항) ① 정보보호담당부서 및 개인정보관리부서는 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.

제 2 장 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 포

함하며, 회사가 고객에게 공급하여 고객 사이트에 위치한 장비 중 회사의 자산에 속하는 것은 정보보호 범위에 포함한다.

제 3 장 정보보호 조직

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.

제 4 장 정보자산 관리

제10조(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.

제11조(정보자산의 분류) ① 정보자산은 그 중요도에 따라 "비밀", "대외비", "일반"으로 분류한다.

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

제12조(정보자산 등급 결정) 각 정보자산의 등급은 생성 시점에 가치와 중요도에 따라 등급을 분류하여 관리한다.

제13조(정보자산의 보호) ① 정보자산은 지정된 장소에 보관되어야 하며, 이용에 대한 통제 절차를 수립

해야 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.

제14조(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.

제 5 장 인적 보안

제15조(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.

제16조(제3자 보안) ① 제3자에게 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.

제17조(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.

제18조(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

제 6 장 관리적 보안

제19조(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.

제20조(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.

제21조(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.

제 7 장 물리적 보안

제22조(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.

제23조(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.

제24조(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.

제25조(사무환경 보안) ① 문서함 등 모든 사무집기는 사용자 책임으로 시건을 철저히 하여 정보의 부당한 유출을 방지하여야 한다.

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

제26조(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.

제 8 장 정보시스템 보안

제27조(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.

제28조(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.

제29조(시스템 계획) 적절한 저장 능력 및 정보처리 능력을 가질 수 있도록 시스템의 처리속도와 사용용량에 대하여 주기적으로 모니터링을 실시하고 이를 기록·관리해야 한다.

제30조(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 해야한다.

제31조(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.

제32조(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.

제33조(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.

제34조(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.

제35조(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.

제36조(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.

제 9 장 접근 통제

제37조(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.

제38조(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.

제39조(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.

제40조(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.

제41조(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.

제 10 장 개인 보안

제42조(패스워드 설정) 회사에서 사용되는 모든 컴퓨터는 부팅 패스워드·로그온 패스워드·화면보호기 패스워드를 설정하여 비인가자가 접근 및 오·남용할 수 없도록 해야 한다.

제43조(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.

제44조(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.

제45조(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.

제 11 장 개인정보 보호

제46조(개인정보보호) ① 제3자를 포함한 회사의 모든 임직원은 업무 수행 시 개인정보보호와 관련된 상위 법규 및 회사 정보보호 정책을 준수하여 개인정보취급업무를 수행해야 한다.

② 모든 개인정보는 사전에 인가된 목적으로만 사용되어야 하며, 용도 외의 임의 목적으로 활용하거나 유출 또는 제공해서는 안된다.

③ 개인정보를 방치되거나 부당하게 유출되지 않도록 그 생산, 유통, 보관, 폐기 등의 전 과정을 철저히 관리하여야 한다.

④ 개인정보보호책임자를 지정·운영하고, 개인정보취급자의 수를 최소한으로 제한하여야 한다.

제 12 장 정보통신 기반시설 보호

제47조(주요정보통신기반시설보호대책의 수립) ① 회사는 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시

설보호대책"이라 한다)을 수립·시행하여야 한다.

② 회사는 제1항의 규정에 의하여 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관(이하 "관계중앙행정기관"이라 한다)의 장에게 제출하여야 한다.

제48조(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

부 칙

제1조 (시행일) 이 규정은 2022년 08월 01일부터 시행한다.