정보보안 경영
시스템 매뉴얼

■ 관 리 본

□ 비 관 리 본

구 분	팀 명 / 직 위	성 명	서 명	일 자
작 성 자	정보보안 관리자	권 찬 우		2024. 02. 14
검 토 자	정보보안최고책임자 /사업책임자	김 성 우		2024. 02. 14
승 인 자	대표이사	김 종 국		2024. 02. 14

(주)대하정보기술

부산광역시 금정구 동천로7번길 63(회동동)

정보보안 경영 시스템 매뉴얼 문서 개정 이력카드				
문서명	정보보안 경영시스템 매뉴얼(Information Security Management Manual)			
개정번호	개정일	개정페이지	개정내용	비고
1.0	2022.02.27	제 정	정보보안 경영 시스템 제정	
2.0	2024.02.14	개 정	정보보안 경영 시스템 재정립	

목 차

정보보호 선언문

정보보호 선언문

㈜대하정보기술의 안정적 운영, 내부정보 및 고객정보보호, 업무연속성 유지 등을 위하여 정보보호관리체계를 구축하고 이를 효율적으로 운영한다.

회사 고객을 위한 정보보호 선언

1.고객에 제공되는 서비스는 상시 제공되어야 하며, 서비스 중단을 최소화 하여야 한다.

2.고객으로부터 제공된 정보는 안전하게 관리/운영되어야 한다.

다음과 같은 원칙을 준수하여야 한다.

1.중요 정보자산은 업무와 무관하게 사용되거나 공개하지 않는다.

2.모든 접근과 변경은 승인을 거쳐야 한다.

3.관련 법규 및 계약에 있어서의 보안 요구 사항을 준수한다.

4.정보유출방지를 위해 모든 임직원은 보안 요구 사항을 준수한다.

대표이사는 다음과 같은 필요한 자원을 적극 지원한다.

1.정보보호를 위한 충분한 예산을 확보하여 지원한다.

2.정보보호를 위해 필요한 조직을 구성하고 충분한 인적자원을 지원한다.

3.정보보호에 필요한 충분한 교육을 지원한다.

4.정보보호를 위해 필요한 정책 지침을 수립하고 시행할 수 있도록 지원한다.

상위 정책 및 지침을 준수하는데 있어 모든 임직원은 성실을 원칙으로 하며, 정보보호관리체계가 지속적으로 유지 발전 할 수 있도록 노력하여야 한다. 또한 본 선언문이 지속적으로 유효성을 가질 수 있도록 년 1회 이상 주기적 검토하고 필요 시 개선작업을 수행 한다.

2024. 01. 02

대표이사 김 종 국

제 1 장 총칙

제1조. 목적

본 규정은 ㈜대하정보기술(이하 '회사') 보안업무 수행에 필요한 원칙과 정보보호 요건을 규정함을 목적으로 하며 상세 운영규정은 하위 세부지침에 따른다.

제2조. 적용범위

본 규정은 회사 정보시스템 자원의 접근 및 보안에 적용되며 내부 임직원, 계약직원 및 외부인력을 그 대상으로 한다.

제3조. 임무의 선언

3-1. 정보시스템 및 서비스를 통하여 생산, 전송, 처리되는 정보와 이에 의하여 제공되는 정보서비스는 회사의 중요한 자산이다.

3-2. 이러한 자산은 그 가치와 중요성에 적합한 수준으로 자연재해, 시스템 및 네트워크의 고장, 내.외부 인원에 의한 우발적이거나 의도적인 각 종의 위협으로부터 보호되어야 한다.

3-3. 회사의 모든 임직원은 본 정책을 이해하고 준수함으로써 정보자산을 보호할 책임이 있다.

제4조. 준용

본 정책 및 세부 하위 지침(이하 '규정')은 "정보통신망 이용촉진 및 정보보호 등에 관한 법률", 동법 시행령, 동법 시행규칙, "개인정보 보호법", 동법 시행령, 동법 시행규칙, "전자상거래 소비자보호법", 동법 시행령, 동법 시행규칙 이하 관련 고시 기준 등의 통제사항과의 일관성을 유지한다.

제 2 장 원칙과 체계

제5조. 정보보호의 대상

정보보호의 대상이 되는 정보자산은 정보화 정보시스템, 정보보호시스템으로 구분되며, 이를 운영하기 위하여 필요한 정보 관련 자산 역시 정보보호의 대상이 된다.

5-1. 정보시스템은 회사에서 관리하는 모든 하드웨어, 소프트웨어 및 네트워크를 말한다.

5-2. 정보보호시스템은 정보의 훼손, 변조, 유출 등을 방지하기 위하여 구축된 시스템을 말한다.

5-3. 정보 관련 자산은 정보 및 정보시스템에 관련된 인력, 시설, 장비, 운영을 위한 절차 및 규정 등을 말한다.

5-4. 정보란 회사가 생산 또는 입수하여 소유하고 있는 것으로 인쇄물 및 컴퓨터나 정

보정장 매체 등에 기록된 전자문서의 형태로 존재하는 것을 말한다.

제6조. 정보보호 요구사항

조직의 정보자산은 다음과 같은 요구사항을 충족하여야 하며 요구사항에 적합한 기능이 제공되고 관리되어야 한다.

6-1. 비밀성 : 정보가 권한이 없는 사람에게 공개되지 않아야 한다. 인가된 사용자만이 주어진 권한에 따라 정보자산에 접근하도록 통제하여야 한다.

6-2. 무결성 : 정보가 불법적으로 변경되지 않고 정확하고 완전하게 유지되어야 한다.

6-3. 가용성 : 권한이 있는 사람이 정보에 대한 접근을 필요로 할 때 적당한 시간 내에 사용 가능해야 한다.

6-4. 준법성 : 저작권법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법, 전자상거래소비자보호법 등의 법적인 요구사항을 준수하여야 한다.

6-5. 책임추적성 : 정보 자산의 소유자, 운영자, 사용자의 역할과 책임을 명확히 하고 책임 추적성을 확보하여야 한다.

제7조. 정보보보조직의 구성 및 역할.책임

정보자산의 정보보호관리업무를 체계적으로 수행하기 위하여 정보보호조직을 구성하고 조직 구성원의 각 직무에 관해 책임과 역할을 정해야 한다.

7-1. 대표이사

7-1-1. 회사의 정보자산을 보호하기 위한 보안 대책을 마련하여야 하며 보안에 대한 총괄 책임을 진다.

7-1-2. 보안의 역할과 책임을 수행하기 위하여 정보보호조직을 구성 운영하여야 한다.

7-2. 정보보호 최고책임자

7-2-1. 정보보호 최고책임자는 대표이사가 지정한 임원이 수행한다.

7-2-2. 회사에 대한 정보보호계획의 전반적인 조정, 검토, 감독 등 보안 총괄 기능을 수행한다.

7-3. 정보보호 관리자

7-3-1. 정보보호 관리자는 회사에 대한 정보보호(개안정보 보호 포함) 업무 관련 관리자로서 보안대책, 보안정책, 지침 개발, 개인정보보호의 각종 보안계획을 수립하고 이행하는 책임을 수행한다.

7-4. 정보보호 담당자

7-4-1. 정보보호담당자는 각 부서별 팀장이 운영보안 담당자업무를 수행한다.

7-4-2. 정보보호담당자는 회사의 정보보호 업무 관련 정보보호관리자를 지원하여 실무를 수행한다.

7-5. 개인정보관리 책임자

7-5-1. 개인정보보호계획과 집행의 전반적인 조정, 검토, 감독 등 개인정보 관련 총괄 기능을 수행한다.

7-6. 개인정보보호관리자

7-6-1. 개인정보보호계획 및 방침의 수립, 개인정보침해 사고 분석, 대응, 개인정보처리 실태관리 결과 및 각종 자료의 취합 등 개인정보보호 관련 업무 전반에 대한 관리 업무를 수행한다.

7-7. 정보보호위원회

7-7-1. 정보보호 관련 최상위 의사결정기구로서 정보보호업무수행을 위한 정책, 지침의 검토 및 승인, 정보보호 자원할당(인력, 예산 등) 등 조직 전반에 걸친 주요한 사안에 대한 검토 및 의사 결정을 수행한다.

7-7-2. 중대 보안 문제 발생 시 대책을 논의하고 처리한다.

7-7-3. 위원장은 정보보호최고책임자가 수행하며, 위원장 부재 시 대표이사가 위원장의 역할을 수행하거나 임시로 지정한 자가 그 역할을 수행할 수 있다. 위원은 각 사업별 소장과 팀장이며, 간사는 정보보호관리자가 수행한다.

7-7-4. 의결은 구성위원의 과반수 이상 출석으로 개최하고, 출석위원 과반수 찬성으로 의결하며, 위원회가 가부동수인 경우 위원장이 결정권을 갖는다.

제 3 장 정보자산의 분류

제8조. 정보자산의 분류

정보자산을 식별하고 조사된 자산의 통제 유지하기 위해 자산의 유형에 따라 정보(문서적 정보와 전자적 정보 모두 포함), 정보시스템서버(서버, PC, 보조저장매체, 네트워크 장비, 응용프로그램, 정보보호시스템 등), 정보 관련 자산(물리적 보안을 위한 시설장비 등)으로 나눈다.

제9조. 정보자산 목록의 유지관리 및 보안등급 정의

식별된 정보자산의 목록을 유지관리하고 보안등급에 따라 안전하게 취급하여야 한다.

9-1. 정보시스템 관련 자산은 기밀성, 무결성, 가용성을 고려하여 '가', '나', '다' 등급으로 분류하며 세부 기준은 "위험관리 지침"을 따른다.

9-2. 정보(문서 및 매체)는 공개될 경우 회사에 미치는 영향 정도에 따라 비밀, 대외비, 일반 등급으로 분류하며 상세 설명은 "문서 및 매체 보안지침"을 따른다.

제10조. 정보자산의 비밀 등급 결정

각 정보의 비밀 구분은 정보 작성자가 정보 생산 시 부여한다. 부여 시에는 정보를 적절히 보호 될 수 있는 최저 등급으로 분류하며 과도 또는 과소 분류되지 않도록 한다. 이에 대한 상세 설명은 "위험관리지침" 및 "문서 및 매체 보안지침"을 따른다.

제 4 장 인원 보안

제11조. 입사 및 퇴사시 보안

인력에 의한 오류, 절도, 사기 또는 설비의 오용에 대한 위험을 감소시키기 위한 절차를 수립 이행하며 상세 설명은 "인적 보안 지침"을 따른다.

제12조. 사용자 교육 및 훈련

정보자산의 사용자가 정보보호 정책을 적극 지원할 수 있도록 하기 위한 절차를 수립 이행 하며 상세 설명은 "정보보호교육 지침"을 따른다.

제 5 장 보안사고 및 장애 관리

제13조. 사고 대응

보안사고의 피해를 최소화하기 위하여 다음 사항이 준수되어야 하며 상세 설명은 "보안사고 대응지침"을 따른다.

13-1. 적합한 관리경로를 통한 신속한 보고절차가 수립되어야 한다.

13-2. 직원은 보안사고 보고절차를 숙지하여야 한다.

13-3. 보안사고나 보안취약점 발견 시 즉각 정보보호관리자에게 보고되어야 하며 신속한 대응이 이루어져야 한다.

13-4. 의심되는 취약점 발견 시 이를 자의적으로 검증하려고 시도해서는 안 된다.

13-5. 보안사고 종결 후 사고의 분석.평가 및 추후 대책 수립 절차가 이행되어야 하며 발견된 취약점에 대해서는 보안 대책이 마련되어야 한다.

제14조. 장애 관리

장애의 피해를 최소화하기 위하여 다음 사항이 준수되어야 하며 상세 설명은 "정보시스템 도안지침"에 따른다.

14-1. 장애 심각도별 대응 방안이 수립되어야 한다.

14-2. 회사 직원은 장애사고 보고절차를 숙지하여야 한다.

14-3. 사고에 대하여 신속하고 적절한 대응이 이루어져야 한다.

14-4. 장애사고 조치 완료 후 심각도별로 담당자에게 보고한다.

제 6 장 물리적 보안

주요 장비 및 설비를 보호하기 위한 물리적 보호구역의 정의, 물리적 접근통제, 주요 장비의 보호 등 물리적 보안 상에 사항은 '물리적 보안지침'을 따른다.

제15조. 보호구역 설정

15-1. 회사의 보안시설, 비밀, 대외비가 있는 장소는 보호구역으로 하며 보호구역은 제한구역과 통제구역으로 나뉜다. 보호구역 정의 및 관리에 대한 상세한 규정은 '물리적 보안지침'을 따른다.

15-2. 보호구역의 등급기준은 다음과 같다.

15-2-1. 통제구역
중요 정보처리설비를 무단 접근, 도난, 파괴 및 업무 방해로부터 물리적으로 보호하기 위하여 물리적 통제 구역을 설정하고 필요한 정보보호대책을 설치한다. 또한 허가된 직원만이 출입할 수 있도록 출입을 통제하고 접근권한을 정기적으로 검토한다.

15-2-2. 제한구역
비교적 중요한 설비나 업무 수행 장소를 말하며 외부자의 접근에 대하여 물리적으로 분리되며 통제가 요구되는 구역이다.

제16조. 장비보안

정보시스템 및 관련 장비를 보안위협과 환경적인 위해 요소로부터 물리적으로 보호하

기 위하여 다음 사항이 준수되어야 한다.

16-1. 장비의 설치 및 보호 : 설치 시에는 불필요한 접근 및 위험을 최소화하도록 배치하고 필요한 통제수단을 도입하여야 한다. 또한 특별한 보호를 요하는 장비는 별도로 분리하여 관리하여야 한다.

16-2. 장비의 폐기 및 재사용 : 중요 정보의 보관장치를 폐기할 시에는 중요 정보를 완전히 삭제한 후 물리적으로 파기하여야 한다. 중요 정보의 보관장치를 재사용할 시에는 중요 정보를 완전히 삭제한 후 재사용하여야 한다.

16-3. 장비 이동의 승인 절차 : 장비가 허가 없이 이동되지 않도록 사전 승인 절차를 거친 후 반출/반입에 관한 이력을 기록하여야 한다.

제17조. 사무실 보안

사무실 내 정보의 무단 접근 및 손상의 위험을 줄이기 위해 자리를 비울 때는 비밀등급의 문서나 저장매체가 책상 위에 놓여 있어서는 안되며 컴퓨터의 화면에 정보에 관한 사항을 남겨놓지 않아야 한다. 중요 정보를 인쇄할 경우 인쇄 즉시 프린터에서 회수하여야 한다. 사무실 보안의 상세 사항은 'PC 보안 지침'을 따른다.

제 7 장 운영 보안

제18조. 정보시스템 운영 절차 및 책임

모든 정보시스템에 대하여 명확한 운영 및 관리절차를 수립하고 적절한 업무분장 체계에 따라 담당자를 지정하여 관리하여야 한다.

제19조. 유해 소프트웨어 방지

소프트웨어와 정보의 무결성을 보호하기 위하여 유해 소프트웨어의 유입을 방지, 탐지 및 대처하기 위한 통제 수단과 절차를 수립하고 관리하여야 한다. 상세 세부사항은 'PC 보안 지침'을 따른다.

제20조. 정보시스템 관리 통제

정보시스템에 대해 적절한 보안관리 및 통제절차를 수립하여 관리하여야 한다. 상세 세부사항은 '정보시스템 보안 지침'을 따른다.

제21조. 문서 및 매체 관리

매체에 저장된 정보를 보호하기 위하여 테이프, 디스크, 카세트 등 각종의 매체에 대한 보관 및 폐기 절차를 수립하고 관리하여야 한다. 상세 세부사항은 '문서 및 매체 보안 지침'을 따른다.

제22조. 응용프로그램 개발 관리 통제

응용프로그램의 개발 시 검토되어야 할 정보보안 통제 사항을 응용프로그램 개발 생명주기별로 통제하여야 한다. 상세 세부사항은 '개발보안 지침'을 따른다.

제23조. 전자거래 보안

23-1. 전자(상)거래서비스 제공 시 안전성과 신뢰성 확보를 위해 관련 법률을 고려하고 보호대책을 수립하여 이행하여야 한다.

23-2. 전자(상)거래사업자와 전자결제업자간에 송.수신 되는 정보에 대해 적절한 보호대책을 수립하여야 하며, 조직 또는 계열사 간 중요정보를 상호 교환하는 경우 안전한 전송을 위한 협약(보안약정서, 계약서, SLA 등)을 체결하고 이행해야 한다.

제 8 장 접근 통제

제24조. 접근통제 개념

정보시스템 및 정보시스템 내에 존재하는 정보에는 승인된 사용자만이 접근할 수 있어야 한다.

제25조. 접근통제 정책

정보보호관리자는 승인 받은 사람만이 정보에 접근할 수 있도록 접근통제 정책을 수립

하고 이에 따라 정보시스템을 통제하여야 한다. 또한 정보시스템에 접근통제 정책의 준수에 필요한 식별 및 인증, 접근통제, 로그 기록 등을 관리하여야 하며, 허가되지 않은 접근을 신속하게 탐지하고 효과적으로 제지하기 위한 대책을 강구하여야 한다.

제26조. 접근통제 절차

정보시스템과 서비스에 대한 접근 권한을 관리하기 위한 절차를 수립.이행 하며 상세 세부사항은 '사용자계정 및 비밀번호 지침'을 따른다.

제27조. 사용자 책임

사용자는 자신의 비밀번호를 안전하게 선택하고 관리할 책임이 있으며, 자신에게 할당된 개인용 컴퓨터의 안전한 관리에 대한 책임이 있다. 또한 공용의 장비 이용에 대한 책임을 인지하고 공용장비 이용 시 관련 지침을 준수하여야 한다.

제28조. 개인정보 보호

개인정보 및 개인정보를 처리하는 정보시스템을 운영함에 있어 개인정보를 체계적으로 관리하여 보호해야 한다. 상세 세부사항은 '개인정보보호 지침'을 따른다.

제 9 장 재해복구 계획

제29조. IT 재해복구 계획의 수립

각종 재해와 비상사태 발생시 신속하고 조직적인 복구 활동을 전개하고, 사후관리를 철저히 하기 위하여 보고체계, 관리부서 및 관리기준을 수립하여 시행하도록 한다. 세부 사항은 'IT 재해복구 관리 지침'을 따른다.

제 10 장 위험평가

제30조. 위험평가의 수행

자체 정보보호 요구사항을 파악하고, 정보자산의 기밀성, 무결성, 가용성, 법적 요구사항을 유지할 수 없게 하는 잠재적인 요소 및 현재 구현된 통제와 취약성 및 위협에 대한 대응이 실패할 수 있는 실제적인 가능성을 파악하여 보다 비용대비 효과적인 대책을 마련하기 위하여 '위험관리 지침'에 준하여 위험평가를 수행한다.

제 11 장 준수 검토

제31조. 정보보호 준수

회사 직원은 정보보호화 관련된 정책, 지침 등을 준수하여야 하며, 지침 준수 시 지침에서 정의한 양식을 준용하되 관리측면에서 필요 시 양식의 작성 목적을 반하지 않는 벙위 내에서 형태를 변경할 수 있다.

제32조. 보안 감사

최소 반기 1회이상 내부 보안 감사를 수행하고 감사결과 지적 사항에 대하여 시정조치를 이행하도록 한다. 상세 세부사항은 '보안감사 지침'을 따른다.

제33조. 법적 요구사항의 준수

정보보호관리자는 관련 법의 변경 등에 대해 법저 요구사항을 검토하여 필요 시 보안통제 방안을 수립하고 정보보로최고책임자에게 보고하여야 한다. 정보보호최고책임자는 이를 정보보호위원회를 통해 검토 후 결정된 조치를 관련 팀에 통보하여 보안통제가 구현되도록 한다.

33-1. 저작권법

33-1-1. 사용자 : 모든 사용자는 사용이 승인된 소프트웨어만을 사용하여야 한다.

33-1-2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 : 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 시행령, 시행규칙 및 기타 관련 고시 기준은 개인정보보호 및 정보통신망의 안정성 확보에 관한 사항을 준수하여야 한다.

33-1-3. 개인정보 보호법 : 개인정보 보호법, 시행령, 시행규칙 및 안정성 확보에 관한

사항을 준수하여야 한다.

33-1-4. 전자상거래소비자보호법 : 전자상거래소비자보호법, 시행령, 시행규칙에 관한 사항을 준수하여야 한다.

제34조. 상벌규정

34-1. 정보보호정책, 제반 지침 또는 절차를 위반하거나, 정보보호책임을 충실히 이행하지 못한 경우 규정에 따라 처벌을 할 수 있으며 상세사항은 '인전보안 지침'에 준하여 시행한다.

34-2. 정보보호책임을 충실히 이행하였을 경우 포상 할 수 있다.

제 12 장 정보보호 활동 평가

제35조. 정보보호 활동 평가 체계

정보보호최고책임자를 포함한 정보보호 관련 담당자의 활동을 정당하게 평가할 수 있도록 연말 인사 고과 시 보안 관련 항목의 평가 기준에 따라 정보보호 조직원들의 활동 성과를 평가할 수 있다.

제 13 장 정보보호정책의 운용

제36조. 정보보호정책의 제.개정

정보보호 정책 및 지침은 회사의 다양한 환경 변화에 따른 정보보호 요구사항이 반영되도록 다음과 같이 정보보호 정책 및 지침을 관리한다.

36-1. 정보보호정책(하위 세부 보안지침 포함)은 정보보호관리자가 주관하여 정기적으로(연 1회) 검토하여 법적 요구사항 및 최신 현황을 고려하여, 필요 시 개정한다.

36-2. 환경 변화에 따른 정보보호 요구사항을 반영하여 새로운 정보보호 지침을 제정할 수 있다.

36-3. 제.개정된 정보보호 정책 및 지침은 정보보호최고책임자 및 정보보호위원회의 승인을 득한다.

36-4. 제.개정된 정보보호 정책 및 지침은 직원이 쉽게 확인할 수 있는 형태로 공지한다.

(부칙)

1. 시행일

본 정보보안 방침은 2022년 07월 20일에 제정되고, 같은 날부터 시행한다.

본 정보보안 방침은 2024년 02월 14일에 부분 개정되고, 같은 날부터 시행한다.