보안규정

1. 목적

본 규정은 ㈜티앤에프(이하 "회사"라고 한다)의 기업비밀을 보호하고 보안 업무를 수행하는데 필요한 제반사항을 규정함을 목적으로 한다. 또한 회사는 Cybersecurity 국제 법규 (UNECE R-155)에 의거 차량 전자장비에 주입되는 Software(이하 "S/W")의 관리를 위해 관리적인 측면의 세부 사항 및 대책, 준수 사항 등에 대하여 정함을 목적으로 한다.

2. 적용범위

본 규정은 회사에 근무하는 전 임직원에게 적용한다. 단, 이 규정에 정한 범위내에서 특수성과 실정에 따라 회사의 출입자, 피교육자, 일용 근로자 및 회사와 계약관련이 있는 특수인에게도 적용할 수 있다.

3. 적용대상

적용 대상은 정보자산을 이용하거나 관리하는 당사 구성원과 관련자 및 외부자로 한다. 적용당사의 생산활동에 수반되어 생산, 보관하는 장치 및 시설물과 기록문서, 복사인쇄물, 도면, 이동식 저장장치(USB), 원재료, 제품 등 기밀정보를 담고 있는 모든 물질을 대상한다.

4. 정보보안 기본수칙

1) 정보자산을 이용, 관리하는 본사 구성원과 관련 외부자는 다음 각 호의 정보 보안 활동의 기본 수칙을 준수하여야 한다.

- 개인별 사용자 계정 및 비밀번호의 기밀을 유지하여야 하며, 본래의 발급 목적으로만 사용하여야 한다.
- 허가받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만 사용하여야 한다.
- 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 아니 된다.
- 정보자산과 연관된 저작권, 특허권 및 소프트웨어 라이선스의 사용 조건을 숙지하고 이를 준수하여야 한다.
- 업무와 관련해 습득한 정보자산을 임의로 외부에 누출해서는 아니 된다.

2) 정보보안 담당부서는 정보통신망과 정보시스템의 안전성 및 정보보안 규정의 준수 여부를 주기적으로 점검하여야 하며 회사 구성원과 관련 외부자는 이에 적극 협조하여야 한다.

3) 정보보안 담당부서는 정보보안 사고를 예방하기 위한 목적으로 정보보안 활동을 즉시 시행할 수 있다.

5. 용어의 정의

이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

No.	용어	정의
1	**정보보호 관리체계**	조직의 주요 정보자산을 보호하기 위해 정보보호 관리절차와 과정을 체계적으로 수립하여 지속적으로 관리·운영하기 위한 종합적인 체계를 말한다.
2	**정보보안**	정보시스템 및 정보통신망을 통해 수집, 가공, 저장, 검색, 송수신되는 정보의 유출, 위변조, 훼손 등을 방지하기 위하여 관리적, 물리적, 기술적 수단을 강구하는 일체의 행위로 사이버안전을 포함한다.
3	**정보시스템**	PC, 서버 등 단말기, 보조기억매체, 전산 통신장치, 정보통신기기, 응용프로그램 등 정보의 수집, 가공, 저장, 검색, 송 수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
4	**정보자산**	회사의 서비스를 제공하기 위한 정보시스템과 정보시스템의 운영·관리에 필요한 시설, 전자정보등 자산을 총칭한다.
5	**기밀성 (Confidentiality)**	비인가자가 임의의 정보를 사용하거나 정보가 노출되지 못하도록 하는 특성으로 자산 또는 데이터가 전송, 백업, 보관 중에 허가 받지 않은 사람에게 노출되지 않아야 함을 말한다.
6	**무결성(Integrity)**	비인가된 방법을 통해 정보를 변경 또는 파괴하지 못하도록 하는 특성으로 정보가 전송되고 저장되는 과정에서 완전성과 정확성을 유지하는 것을 말한다.
7	**가용성(Availability)**	권한을 가진 개체의 요구에 따라 정보자산을 지속적으로 접근하고 사용이 가능하도록 하는 특성을 말한다.
8	**중요정보**	노출, 변경, 파괴 시 업무에 중대한 영향을 미칠 수 있는 정보로서, 암호화 대상은 개인정보보호법에 따른다.
9	**보안자료**	정보자산 중 전산화 되어 파일로 존재하거나 출력되어 문서로 존재하는 자료로써, 외부에 유출되는 경우, 회사의 경영상 기술상의 손실이 발생할 수 있는 자료를 의미한다.

6. 보안관리의 주체

보안관리	보안관리의 총괄책임자는 대표이사 또는 대표이사가 권한을 위임한 임원급 관리자로 정할 수 있다. 보안관리는 부서단위로 하는 것을 원칙으로 하며 이 때 보안관리의 주체는 보안책임자 및 보안관리 보안담당자로 한다. - 보안책임자 : 각 부서의 최고 지위자로 하며, 필요시 차하위자에게 위임이 가능하다. - 보안담당자 : 보안책임자의 임명으로 보안에 대해 전반적인 관리를 담당하는 자를 말하며 과장급 이상 관리자로 선정하되 필요시 차하위자에게 위임이 가능하다.
물리적 보안	비인가자로부터 회사의 시설 및 인원을 보호하기 위한 출입통제, 정보자산의 반.출입 통제, 상황모니터 등의 보안활동을 의미한다. - 상황모니터 : 사업장내 설치된 CCTV 또는 경비인력 운영을 통해 안전, 사고 및 보안현황을 실시간 확인하는 것에 관련한 활동을 의미한다. - 출입 통제 설비 : 사업장 내의 출입 인원의 신원을 확인하여 비인가 인원의 사업장내 출입 통제를 목적으로 하며 인가 인원의 출입 이력을 확인할 수 있는 기기를 의미 한다.
관리적 보안	보안 조직 구성 및 운영, 보안정책 및 절차관리, 보안교육, 보안점검, 보안사고조사 등의 보안활동을 의미한다. - 총괄 보안책임자 : 회사의 대표로부터 정보보호에 대한 권한을 위임 받아 전사 보안책임자 의결사항에 대하여 최종 승인할 수 있는 권한을 갖는다. - 전사 보안책임자 : 경영지원부장이 담당하며 보안 조직 프로세스 승인, 수행업무 관리감독, 보안 유관업무 승인 등의 업무를 담당한다. - 전사 보안관리자 : 경영정보팀장이 담당하며 회사의 보안관리 총괄, 부문별 보안업무 조정 및 협의체 등 보안조직 운영 등의 업무를 담당한다.
기술적 보안	S/W 보호 및 정보 시스템을 통한 유출을 예방하기 위한 운영관리, 정보 시스템 접근통제, 개발 및 유지 보수, 침해사고관리 등의 보안활동을 의미 한다. - 정보시스템 : 사용자에게 원활한 서비스의 제공을 목적으로 하는 하드웨어 일체와 주변장치 및 운영체제를 포함한 각종 시스템 소프트웨어 및 DBMS를 총칭한다. - 네트워크 : 회사의 사업을 영위하기 위해 사업장간에 송수신되는 정보 혹은 관련기관 간에 주고받는 각종 정보를 전달하여 주는 시스템들을 다양한 형태로 연결시켜 주는 유무선 통신망을 의미한다. - 백업 : 예상치 못하고 바람직하지 않은 사건에 의해 발생할 수 있는 정보서비스 혹은 정보자산의 손상을 최소화하고 이를 복구하기 위해 필요한 복사본을 만드는 것을 말한다.

- 복구 : 사전에 백업 받았던 복사본을 이용하여 이전의 상태로 전환하기 위한 RECOVERY와 단순히 백업받았던 자료를 재설치하는 RESTORE 작업을 총칭하여 말하며, 복구를 위해서는 반드시 백업이 선행되어야 한다.

- 단말기 : 전산시스템의 입출력 장치를 말하며, LAN 혹은 WAN으로 연결된 개인용 PC 및 프린터, 콘솔, 스캐너 장비 등이 포함된다.

- PC : 데스크탑과 노트북을 말한다.

- 모바일기기 : 휴대폰, 스마트폰, PDA, 태블릿 등을 말한다.

- 정보보안사고(침해사고) : 보호관리 대상에 속하는 정보 및 정보시스템이 무단으로 파괴되거나, 유출, 변조되어 정보보안관리체계에 문제가 발생하는 경우를 말한다.

- 웹메일 : 로그인과 로그아웃의 과정을 거쳐 웹 브라우저를 이용해서 메일을 보낼 수 있는 방식의 메일 서비스를 말한다.

- VPN (Virtual Private Network) : 인터넷과 같은 공중망을 사용하여, 사설망을 구축하게 해주는 기술 혹은 통신망의 총칭이다.

- P2P (Peer to Peer) : 인터넷상에서 이루어지는 개인 대 개인의 파일공유 기술 및 행위를 말한다.

- 웹하드, 웹폴더 : 인터넷을 통해 모든 형태의 자료를 보관, 이동, 공유하거나, 파일의 보관, 업로딩 및 다운로딩이 가능한 정보 저장 서비스를 말한다.

- DMZ (Demilitarized Zone) : 방화벽 구성 시 외부로 노출되어야 할 서버나 PC 등을 위해 구성된 네트워크 영역을 말한다.

- FTP (File Transfer Protocol) : 인터넷을 통하여 어떠한 컴퓨터에서 다른 컴퓨터로 파일을 송수신 할 수 있도록 지원하는 프로토콜을 말한다.

- LAN (Local Area Network) : 범위가 그리 넓지 않은 일정 지역 내에서 다수의 컴퓨터나 OA기기 등을 속도가 빠른 통신선로로 연결하여 기기간에 통신이 가능하도록 하는 근거리 통신망을 말한다.

- IP (Internet Protocol) Address : 인터넷을 사용할 때 단말기에 할당되는 고유한 주소를 말한다.

- 공중망 (Public Network) : 불특정 다수에게 서비스 할 수 있도록 통신업체들이 구축한 통신망으로 일반적인 인터넷 망을 말한다.

- 사설망 (Private Network) : 기업이나 학교 등의 특정 기관에서 사용하기 위하여 구축한 통신망을 말하며, 외부에서는 VPN 등 특정 방법을 사용하지 않는 한 접근이 되지 않는다.

- WAN(Wide Area Network) : 지리적으로 멀리 떨어져 있는 넓은 지역을 연결하는 통신망을 말하며, LAN보다 속도가 느리다.

7. 보안책임자 및 보안관리자의 임무

본 보안규정의 제2조 (적용 범위) 규정의 적용을 받는 업체의 보안 관리 책임자는 제3조 (적용 대상) 규정의 적용을 받는 대상자에 대한 전반적인 책임을 가지며, 그 해당 소속의 인원은 이를 보안유지 하고, 보호하여야 할 책임이 있다. 보안 관리 담당자는 보안 관리 책임자의 명을 받아 본 규정의 적용, 운용, 집행 및 관리 전반에 대한 실무권한을 가지며, 효율적인 보안업무 수행에 필요한 지원업무를 성실히 수행할 책임이 있다. 보안사고 발생시의 책임은 사고 당사자 또는 유발자가 우선하며, 해당 소속부서 비밀보관 책임간부 및 임원이 연대책임을 져야 한다.

1) 보안책임자는 다음 각 호에 정한 임무를 수행한다.

- 각종 비문의 보안성 검토 및 비밀등급의 결정
- 일일보안점검 및 각종 시건상태의 확인 감독
- 부서내 직원의 퇴직시 필요한 보안조치
- 부서내의 보안담당자 임명

2) 보안담당자는 다음 각 호에 정한 임무를 수행한다.

- 부서의 보안업무 활동계획 수립 및 시행
- 부서원의 보안활동 지도, 감독
- 부서의 보안관련 서류 유지, 관리
- 부서내의 통신 및 컴퓨터 보안 관련사항 일체