정보보안 및 개인정보보호 정책

1. 총칙

1.1. 목적

본 정책은 주식회사 엘지씨엔에스(이하 '회사')와 회사의 서비스를 이용하는 고객의 중요 정보 자산을 보호하기 위한 정책으로 관련 법규에 대응하고, 정보의 오남용, 훼손, 변조, 유출 등의 위협으로부터 중요 정보를 보호하기 위한 정보보안 및 개인정보보호에 필요한 제반사항을 정함에 그 목적이 있다.

1.2. 적용범위

1.2.1 본 정책은 회사에 근무하는 모든 임직원, 외부자, 제3자를 포함하여 적용한다.

1.2.2 본 정책은 회사가 보유한 유·무형의 모든 자산 및 임직원, 고객 및 협력업체의 개인정보 등 인적자원에 의해 파생된 자산과 활동 전체를 포괄하여 적용한다.

2. 정보보안 관리방침

2.1. 정보보안 정책 관리

경영진의 의지와 정보보안의 방향성을 선언적으로 담고 있는 규정과 정보보안 영역별로 구분된 세부규칙을 수립하고, 관련 법령 및 규제, 국제 표준에 부합하도록 지속적으로 점검하고 개선한다.

2.2 정보보안 조직

2.2.1 정보보안 관리활동을 체계적으로 이행하기 위하여 전사 정보보안 업무를 총괄하는 정보보호・개인정보보호 최고책임자, 정보보안・개인정보보호 주관부서, 유관부서, 부서별 책임자 및 담당자로 조직을 구성한다.

2.2.2 정보보안 관련 협의·조정·계획 및 실적 등에 관한 원활한 업무 수행을 위해 정보보호위원회와 정보보안협의회를 구성 및 운영한다.

2.3 정보자산 식별 및 보안관리

2.3.1 모든 정보자산(서버, PC, 네트워크, 문서 등)에 대해 식별·분류·등급평가를 실시하고, 위험평가를 통해 위협을 식별하여 보호대책을 적용한다.

2.3.2 정보시스템 개발·운영·폐기 전 과정에서 보안 요구사항을 반영하고, 접근통제·암호화·백업 등 보호조치를 시행한다.

2.4 인적/물리 보안

2.4.1 임직원 및 외부자에 대한 보안 교육·서약·권한관리 등을 실시하며, 정보유출 방지 대책을 적용한다.

2.4.2 보호구역을 설정하고, 보호구역에 대한 출입통제, 영상정보처리기기 설치 등 물리적 보호조치를 적용한다.

2.5. 클라우드 보안

2.5.1 회사는 클라우드 서비스 도입 시 물리적 위치, 데이터 등급, 관리 및 운영수준을 기준으로 서비스유형을 선정하고, 보안 요구사항을 반영하여 서비스 계약을 체결한다.

2.5.2 클라우드 표준 보안 아키텍처를 준수하여야 하며, 신규 가상자산의 생성 및 변경관리부터 운영종료 절차에 이르기까지 체계적인 보안관리 방안을 마련한다.

2.6 정보보안 점검 및 감사

2.6.1 회사는 정기적인 점검활동을 수행하여 국내외 정보보안 · 개인정보보호 관련 법률 및 회사의 정책에 위배되는 사항이 없는지 확인하고 개선해야 한다.

2.6.2 정보보안 · 개인정보보호 주관부서는 정기/비정기 점검 및 감사 활동을 통해 정책의 준수여부를 확인하고, 필요시 대책을 마련한다.

2.7 정보보안교육

2.7.1 정보보안 주관부서에서는 임직원 및 외부자의 정보보안 인식 제고를 위한 정보보안 · 개인정보보호 교육 프로그램을 운영한다.

2.7.2 주기적으로 정보보안 · 개인정보보호 교육을 실시하며, 교육 방법, 교육 대상, 교육 내용 등의 사항을 포함하여 교육 계획을 수립하고 수행결과를 분석하여 개선한다.

3. 개인정보보호

3.1 전사 개인정보의 보호

3.1.1 개인정보 처리 기준, 정보주체 권리 보장 등의 다음 각 호의 사항을 준수한다.

1) 개인정보의 내부관리계획 수립·시행
2) 개인정보 처리 기준
3) 정보주체 권리보장
4) 개인정보 안정성 확보조치 적용
5) 익명·가명정보 보호
6) 영상정보처리기기 설치·운영
7) 개인정보 유출 통지 및 신고

3.1.2 개인정보보호 주관부서는 개인정보보호 법령에서 규정된 사항을 정기적으로 검토하고 개선한다.

3.2 개인정보보호 기본원칙

1) 무분별한 개인정보 수집 자제
2) 개인정보 수집 시 필수정보와 선택정보 구분
3) 주민등록번호 등 고유식별정보와 종교, 건강정보 등 민감정보는 원칙적 처리금지
4) 홍보·판매 목적으로 개인정보 위탁 시 고객에게 고지하고 철저히 관리
5) 개인정보는 데이터 암호화 등 안전한 방법을 사용하여 처리
6) 개인정보 보관 시 법령에서 정한 보유기간 준수
7) 개인정보 수집목적 만료 시 알아볼 수 없도록 파기
8) 영상정보처리기기에는 반드시 안내판 설치
9) 개인정보보호에 관한 지침·문서 등을 반드시 구비
10) 정보주체의 권리보장 및 개인정보유출, 집단분쟁조정, 단체소송에 대비

4. 보안사고 대응

4.1 보안사고 대응 체계 및 사후 관리

4.1.1 보안사고 대응 절차를 수립하고, 보안사고 발생 시 절차에 따라 사고에 대응한다.

4.1.2 보안사고 발생 시 체계적이고 효율적인 대응을 위해 사고 대응 훈련 및 교육을 주기적으로 실시하여, 대응 체계를 지속적으로 개선한다.

5. 재해복구

5.1 체계구축 및 사후관리

5.1.1 신속한 복구를 위한 재해복구체계에는 유관부서 및 정보보안 주관부서 등을 포함한 재해복구팀을 구성하고 책임과 역할을 정의한다.

5.1.2 업무영향분석을 통해 복구 우선순위와 복구 목표를 설정하고 적절한 시간 내에 복구할 수 있는 체계를 구축한다.

5.1.3 재해복구계획에 따른 전략과 대책이 복구 목표를 달성할 수 있도록 정기 훈련을 실시한다.