서진시스템 ESG 정책

정보보호 및 개인정보보호 정책

Data Protection and Privacy Policy

Innovating Sustainably, Manufacturing Responsibly.

지속가능한 혁신, 책임감 있는 제조

SEOJIN SYSTEM

정보보호 및 개인정보보호 정책

Data Protection and Privacy Policy

정보보호 및 개인정보보호 정책 Data Protection and Privacy Policy

1. 목 적

본 정책은 서진시스템 및 그 모든 사업장(자회사, 계열사 등)이 경영활동 전반에서 정보자산과 개인정보를 안전하게 보호하고, 법적·윤리적 책임을 성실히 이행하기 위해 필요한 원칙과 기준을 수립하고 정보의 기밀성, 무결성, 가용성을 보장하는 것을 목적으로 한다.

2. 적용 범위

본 정책은 서진시스템 및 그 모든 사업장(자회사, 계열사 등)과 임직원에게 동일하게 적용한다. 또한, 회사와 관련된 모든 정보 자산 및 이를 이용한 모든 업무에 적용되며 회사와 계약관계에 있는 제3자, 협력회사 및 기타 비즈니스 파트너, 기타 출입자에게도 본 정책을 준수하도록 요구한다.

3. 기본 원칙

3.1 법령 및 국제 기준 준수

- 정보보호와 개인정보 보호에 관한 국내외 모든 법령 및 국제 기준을 성실히 준수한다.
- 대한민국의 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등 국내 관련 법령은 물론, 유럽연합 일반 데이터 보호 규칙(General Data Protection Regulation) 등 정보보호 관련 국제 기준을 존중하고 준수한다.
- 기업 활동 중 수집, 보유, 활용되는 모든 정보가 적법하게 관리되도록 노력한다.
- 조직의 내부 관행이나 외부 이해관계자의 요청은 정보보호 및 개인정보보호 위반을 정당화하는 사유가 될 수 없다.

3.2 정보보호에 대한 책임 있는 인식

- 모든 임직원은 정보보호의 주체로서 책임감을 가지고 조직의 정보자산 보호에 적극 참여한다.
- 정보보호는 전사적 가치로, 모든 업무 수행에서 정보보안과 개인정보 보호 원칙을 고려한다.

3.3 정보자산의 보호

- 회사는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 정보보호 활동의 핵심 원칙(CIA)로 인식하며, 모든 보안정책과 기술적 통제는 이 세 가지 가치 실현을 목표로 설계 및 운영된다.
- 회사의 핵심기술, 내부 문서, 시스템, 네트워크 등 모든 정보자산은 외부 유출, 무단 접근, 파괴 등 위험으로부터 보호되어야 하며, 적정한 수준의 기밀성, 무결성, 가용성이 유지되어야 한다.

정보보호 및 개인정보보호 정책 Data Protection and Privacy Policy

3. 기본 원칙

3.4 개인정보 보호

- 개인정보는 수집 목적이 명확해야 하며, 그 목적에 필요한 범위 내에서 최소한으로 처리되어야 한다.
- 개인정보의 이용, 보관, 파기 전 과정에서 정보주체의 권리와 사생활 보호가 최우선으로 고려되어야 한다.

3.5 정보보호의 윤리적 원칙

- 정보는 정당한 목적 하에 적법하고 투명하게 사용되어야 하며, 타인의 권리를 침해하거나 부당한 이익을 추구하는 수단으로 악용되어서는 안 된다.
- 내부 정보와 시스템 접근 권한은 업무 목적 외 사용을 금지하며, 무단 열람, 저장, 복제, 전달 행위는 금지된다.

4. 실행 방안

4.1 정보보호 관리체계 운영

- 정보시스템의 안정적 운영을 보장하며, 보안사고로부터의 산업상 손실을 최소화하기 위한 정보보호 관리체계를 구축 및 운영한다.
- 정보보호와 관련된 업무 절차, 권한 관리, 시스템 접근 통제를 통해 중요 정보자산의 기밀성, 무결성, 가용성을 유지한다.
- 사이버 보안 사고, 내부 정보 유출 등 주요 위험을 사전에 예방하고, 사고 발생 시 신속하게 대응할 수 있도록 조치 체계를 마련한다.

4.2 개인정보 보호 관리

- 개인정보는 수집·보유·이용·파기 전 과정에서 최소한의 범위 내에서 적법하게 처리되며, 정보주체의 권리를 존중하는 방향으로 관리한다.
- 개인정보의 안전한 처리를 위해 가능한 기술적·관리적 보호조치를 검토하고, 단계적으로 도입한다.
- 개인정보 취급자가 개인정보 처리 원칙을 이해할 수 있도록 기본 교육을 운영하며, 외부 열람 및 오·남용을 방지하기 위한 내부절차를 구축한다.

정보보호 및 개인정보보호 정책 Data Protection and Privacy Policy

4. 실행 방안

4.3 임직원 교육 및 정보보호 인식 제고

- 모든 임직원이 정보보호 및 개인정보 보호의 중요성을 인식하고, 관련 규정을 숙지할 수 있도록 교육을 정기적으로 시행한다.
- 개인정보 취급 업무 담당자에게는 별도 교육을 실시하여 정책 이행 역량을 강화한다.

4.4 담당부서 운영 및 역할

- 정보보호 및 개인정보 보호에 관한 정책과 이행 사항은 지정된 전담 부서(또는 책임자)가 총괄하며, 이행 여부를 모니터링하고 주요 개선사항을 관리한다.
- 필요 시 외부 자문을 통해 정보보호 체계의 적정성을 검토하고, 업무 부서와 협력하여 조치를 시행한다.
- 본 정책은 정보보호 최고책임자(CISO), 정보보호 관리자, 정보보호 담당자로 구성된 정보보호 조직의 책임과 역할을 다음과 같이 규정한다.

> **정보보호 최고책임자(CISO)**
> 정보보호 계획, 규정, 지침 등 정보보호 관련 주요 사항의 검토 및 승인, 조직 내 정보보호 정책 수립과 관리 체계를 총괄
>
> **정보보호 관리자**
> 정보보호 계획 및 규정의 작성, 정보보호 지침 수립 및 이행 관리, 전사적 정보보호 활동의 실무적 조율
>
> **정보보호 담당자**
> 정보보호 관리체계의 유지·운영, 보안 점검 및 개선 활동, 사고 대응 등 정책 실행을 위한 실무 업무 수행

- 조직 규모나 업무 특성에 따라, 최고책임자는 각 부서 또는 사업장별 정보보호 담당자를 지정할 수 있으며, 이들은 소속 부서 내 정보보호 활동을 효율적으로 수행한다.

4.5 사고 대응 및 위반 시 조치

- 임직원은 정보보호 및 개인정보 침해 사고 또는 이상 징후를 인지한 경우, 지정된 보고 채널을

정보보호 및 개인정보보호 정책 Data Protection and Privacy Policy

4. 실행 방안

통해 즉시 알릴 책임이 있다.

- 고의적이거나 중대한 위반 행위에 대해서는 관련 규정에 따라 징계 등 적절한 조치를 취할 수 있다.

4.6 기술적 · 물리적 보안 강화

- 회사는 정보자산의 기밀성, 무결성, 가용성을 확보하기 위하여 방화벽, 침입 차단 및 탐지, 암호화, 자산관리 등 다양한 기술적 보안조치를 도입·운영한다.
- 임직원 단말기 및 시스템에 대한 보안성 점검을 정기적으로 실시하며, 악성코드 방지 및 자산 통제를 위한 기술적 조치를 시행한다.
- 필요 시 주요 시설에 대해 출입 통제, CCTV 등 물리적 보안수단을 적용하여 비인가 접근을 방지한다.

문서 제정 및 개정 기록

담당부서 : 정보전략팀

No	개정 번호	개정된 페이지	개정 내용	개정일
1	0	0	최초발행	24/06/2025
2				

SEOJIN SYSTEM