# [두산에너빌리티 정보보호 정책]

## 1. 정보보호 전략 및 정책

두산에너빌리티는 고객의 신뢰를 최우선 가치로 삼으며, 정보보호를 기업의 핵심 책임으로 인식하고 있습니다. 이를 위해 ISO 27001 국제 표준을 기반으로 한 명확한 정보보호 정책을 수립하여 전사적으로 운영하고 있습니다. 정보보호 정책은 클라우드 환경에서의 데이터 유출, 내부자의 부주의, 공급망 내 보안 취약점 등 다양한 리스크를 체계적으로 식별하고, 이에 대한 구체적인 대응 전략을 마련합니다. 또한 모든 임직원은 정보보호 정책을 숙지하고 준수할 의무가 있으며, 외부 협력사와의 계약 시에도 동일한 수준의 정보보호 기준을 요구하여, 제3자로부터의 위협도 철저히 통제하고 있습니다.

정보보호 정책은 경영진의 정기적인 검토를 통해 최신화하고 있으며, 회사의 모든 보안 활동의 기준이 됩니다.

## 2. 정보보호 조직 및 체계

두산에너빌리티는 정보보호의 체계적 운영을 위해 최고정보보호책임자(CISO)를 중심으로 한 전담 조직을 구성하고 있습니다. CISO는 정보보호 정책의 수립과 실행을 총괄하며, 개인정보보호책임자(CPO)를 겸임하여 법적·윤리적 책임을 다하고 있습니다. 정보보호 전담부서는 정책 운영, 시스템 점검, 사고 대응, 임직원 교육 등 실무를 담당하며, 각 부서와 긴밀히 협력하여 전사적 보안 체계를 유지합니다.

모든 임직원은 자신의 업무에 맞는 정보보호 책임을 지니고 있으며, 계정 관리, 이상행위 인지 및 신고, 민감정보 취급 등 세부 절차를 준수합니다. 외부 협력업체 역시 사전 보안점검과 계약서 내 필수 보안 조항을 통해 관리되며, 이를 통해 외부 리스크도 효과적으로 통제하고 있습니다.

## 3. 정보보호 인프라

두산에너빌리티는 안전한 디지털 환경 조성을 위해 다양한 보안 시스템을 도입하고, 기술과 정책을 지속적으로 개선하고 있습니다. 정기적인 위험 평가를 통해 방화벽, 침입차단시스템, 접근제어, 암호화, 이중 인증 등 다양한 보호 장치를 운영하고 있습니다. 특히 중요 데이터는 암호화하여 저장하고, 변경 이력 및 복구 체계를 갖추어 무단 수정이나 손실을 방지합니다. 민감 정보는 보안 등급에 따라 분류하여 관리하며, 저장부터 폐기까지 전 주기 동안 보호조치를 적용합니다. 내부 감사와 외부 점검 결과는 시스템 개선에 적극 반영되며, 새로운 위협이 발견될 경우 신속하게 대응할 수 있도록 인프라를 유연하게 관리합니다. 이러한 노력은 데이터 무결성과 보호를 보장하는 기반이 됩니다.

## 4. 정보보호 인증·평가 및 활동

두산에너빌리티는 국제 정보보호 관리체계인 ISO 27001을 바탕으로 보안 수준을 객관적으로 점검받고 있습니다. 24시간 365일 운영되는 글로벌 보안관제센터(GSOC)를 통해 정보보호 위협을 실시간 모니터링하고, 이상행위나 침해 시도에 즉각 대응합니다. 만약 침해사고가 발생할 경우, 사전에 마련된 대응 매뉴얼에 따라 신속히 조치하며, 사고 원인 분석과 재발 방지까지 체계적으로 관리합니다.

임직원은 연 1회 이상 정보보호 교육을 받고, 피싱 모의 훈련 등 다양한 캠페인을 통해 보안 인식을 높이고 있습니다. 외부 협력사에 대해서도 정기적인 보안 점검과 보안 협약 이행 여부 확인을 통해 제3자로부터의 위협을 예방하고 있습니다. 이러한 활동들은 회사의 정보보호 시스템을 지속적으로 개선하고, 안전한 업무 환경을 유지하는 데 중요한 역할을 합니다.