정보보안경영 정책

[정책 관리 정보]

제정 일시 : 2025년 11월 1일

주관 부서 : 인사총무Part

결재 승인 : 대표이사(CEO)

1. 목적

본 정책은 LS머트리얼즈(이하 "회사"라 한다)의 기밀정보 및 정보자산을 보호하고, 정보의 기밀성·무결성·가용성을 확보하기 위한 기본 원칙과 준수사항을 규정함을 목적으로 한다.

2. 적용대상 및 범위

1) 본 정책은 ISO27001 도입 및 운영에 따라 회사 전 임직원을 포함한 이해관계자 전체에 적용한다.
2) 회사 출입자(방문객), 협력·용역업체, 파견/상주인력 등 회사 정보자산을 취급하는 자에게도 계약/안내를 통해 준용될 수 있다.
3) 관계 법령(예: 개인정보보호법) 및 국가 연구개발 과제 보안지침 등 상위 규정이 우선하며, 상충 시 관련 법령/지침을 따른다.

3. 정보보안 기본원칙

1) 업무상 필요 최소한(Need-to-Know) 원칙에 따라 정보 접근 및 취급을 제한한다.
2) 회사 정보자산은 회사 목적(정상적인 업무수행) 범위에서만 사용한다.
3) 승인되지 않은 방식의 외부 공개·전송·반출을 금지한다.
4) 보안사고 의심 징후(유출·해킹·분실·침입 등)를 인지하면 즉시 보고한다.
5) 회사는 법령 및 내부 기준에 따라 정보자산 보호를 위한 관리적·기술적·물리적 보호조치를 운영한다.

4. 역할과 책임

1) 경영진/총괄보안책임(CISO) : 전사 보안정책 수립, 보안조직 운영, 사고 대응 총괄
2) 보안 주관부서(보안관리부서) : 지침 운영/개선, 교육·점검, 사고 조사 지원
3) IT 운영부서 : 시스템·네트워크·서버 등 정보시스템 보안 운영 및 기술적 조치
4) 각 부서장 : 부서 내 보안 준수 관리, 인원·자산 변동 시 통제, 외부인 출입/자료취급 관리
5) 임직원 및 협력사 인력 : 지침 준수, 계정/비밀번호 보호, 의심사례 즉시 신고

5. 문서 및 정보 취급

1) 회사 업무로 생성/취득한 문서·자료는 회사 자산이며, 보호조치 없는 대외 반출(게시/전달/발송 포함)을 금지한다.
2) 비밀정보는 지정된 승인 체계에 따라 분류·관리하며, 표시/보관/배포/폐기 기준을 준수한다.
3) 비밀정보는 관련자 외 열람·취급을 금지하며, 불필요한 복제·복사를 제한한다.

5. 정보보안 위험관리

1) 회사는 정보자산을 식별하고, 정보자산에 대한 위협 및 취약점을 고려하여 정기적으로 정보보안 위험평가를 수행한다.
2) 위험평가 결과에 따라 위험의 수용·감소·회피·전가 등 적절한 위험처리 방안을 수립·이행한다.
3) 신규 시스템 도입, 조직·업무 변경 등 중요한 변화가 있는 경우 위험평가를 재수행한다.
4) 위험관리 활동의 결과는 문서화하여 관리하고, 그 결과를 경영진에 보고한다.

6. 문서 및 정보 취급

1) 회사 업무로 생성/취득한 문서·자료는 회사 자산이며, 보호조치 없는 대외 반출(게시/전달/발송 포함)을 금지한다.
2) 비밀정보는 지정된 승인 체계에 따라 분류·관리하며, 표시/보관/배포/폐기 기준을 준수한다.
3) 비밀정보는 관련자 외 열람·취급을 금지하며, 불필요한 복제·복사를 제한한다.
4) 비밀문서는 분실·방치되지 않도록 분리 보관, 잠금, 접근제어 등 보호조치를 적용한다.
5) 출력물 및 저장매체(CD/USB 등)는 승인된 절차와 보호조치 하에 취급하며, 불필요 시 안전하게 폐기한다.

7. 출입 및 물리보안

1) 회사 사업장 및 주요 시설은 보안 수준에 따라 구역을 구분하고 출입을 통제한다.
2) 방문객은 사전 등록 및 안내 절차를 원칙으로 하며, 허가된 범위 내에서만 출입한다.
3) 임직원·외부인 모두 사원증/출입증 등 식별수단을 준수하며, 무단출입 및 출입수단의 대여·도용을 금지한다.
4) 촬영/녹음/저장 기능이 있는 기기 및 휴대용 저장매체는 회사 기준에 따라 반입·사용이 제한될 수 있다.

8. 휴대용 저장매체(USB 등) 및 장비 관리

1) 휴대용 저장매체는 회사 기준에 따라 등록·승인된 경우에 한해 업무 목적 범위에서 사용한다.
2) 개인 소유 저장매체의 무단 반입·사용 및 회사 정보의 무단 저장·반출을 금지한다.
3) 업무상 불가피한 반출입은 사전 승인 및 보호조치(암호화 등)를 준수한다.

9. 정보시스템 보안

1) 모든 시스템 접근은 업무 역할 기반 권한에 의해 승인된 사용자만 가능해야 한다.
2) 계정은 개인별로 부여하며 공유를 금지한다.
3) 비밀번호는 안전한 기준(추측곤란, 주기적 변경 등)을 준수하고, 노출 의심 시 즉시 변경한다.
4) 악성코드 예방을 위해 보안 업데이트, 백신 등 보호조치를 유지하며, 의심 징후 발견 시 즉시 신고한다.
5) 외부에서 내부로의 접속은 회사가 승인한 보호대책 하에 제한적으로 허용한다.
6) 중요 데이터는 필요 시 암호화 및 백업을 수행하고, 변경은 승인된 권한자에 의해 수행한다.

10. 이메일·인터넷 사용

1) 인터넷 사용은 업무 목적 범위 내에서만 허용하며, 회사 정책에 반하는 사이트/행위는 제한될 수 있다.
2) 개인 웹메일의 업무 사용은 제한될 수 있으며, 회사 이메일 계정은 정책에 따라 관리된다.
3) 회사 정책·비밀정보·법령 위반 소지가 있는 자료를 이메일로 무단 발송하는 행위를 금지한다.

11. 협력업체·공급망 보안

1) 회사는 업무를 위탁하거나 회사 정보자산에 접근하는 협력업체에 대하여 회사에 준하는 정보보호 수준을 요구한다.
2) 협력업체와 계약 시 보안 준수 의무, 비밀유지, 정보자산 보호 및 사고 발생 시 책임에 관한 사항을 명시한다.
3) 회사는 협력업체의 보안 준수 여부를 정기적으로 점검하고, 필요한 시정조치를 요구할 수 있다.
4) 위탁 업무 종료 시 제공한 정보자산의 반납·파기 등 필요한 보호조치를 이행하도록 한다.

12. 보안교육 및 점검

1) 회사는 임직원의 보안 인식 및 역량 강화를 위해 정기 교육과 안내를 실시한다.
2) 회사는 정보보호 수준 유지를 위해 보안 점검/진단을 수행할 수 있으며, 필요한 시정조치를 요구할 수 있다.
3) 협력사 및 외부 인력은 계약 및 안내된 보안 준수사항을 이행해야 한다.

13. 정보유출 예방 및 모니터링

1) 회사는 법령이 허용하는 범위 내에서 정보자산 보호 및 사고 예방을 위해 업무용 정보시스템 사용기록 등을 점검·관리할 수 있다.
2) 모니터링/점검을 통해 알게 된 정보는 보안 목적 외 사용을 금지하며 관련 법령과 내부 기준을 준수한다.
3) 관련 대상자에게는 필요한 범위에서 사전 고지/동의를 받을 수 있다.

14. 보안사고 대응

1) 보안사고(의심 포함) 발생 시 임직원 및 관련자는 즉시 보안 주관부서/IT부서 등 지정 창구로 보고한다.
2) 회사는 사고 확산 방지, 원인 조사, 복구 및 재발 방지 조치를 수행한다.
3) 법령상 신고·통지 의무가 있는 사고는 관련 법령에 따라 조치한다.

15. 위반 시 조치

본 지침 및 회사 보안규정 위반 시 회사는 내부 기준 및 관계 법령에 따라 접근권한 제한, 계약상 조치, 징계 및 민·형사상 조치를 포함한 필요한 조치를 할 수 있다.

16. 법규 준수 및 지속적 개선

1) 회사는 정보보호와 관련된 법령·규제 및 계약상 요구사항을 식별하고 이를 준수한다.
2) 회사는 정보보호경영시스템의 적합성과 효과성을 확인하기 위하여 정기적으로 내부심사를 수행한다.
3) 경영진은 정기적으로 정보보호경영시스템의 운영 결과를 검토(경영검토)하고 개선 사항을 결정한다.
4) 회사는 점검·심사 및 사고 분석 결과를 반영하여 정보보호 활동을 지속적으로 개선한다.

17. 준수 서약 및 협력

1) 임직원 및 필요한 외부 인력은 회사가 정한 보안 서약/동의 절차를 이행할 수 있다.
2) 회사와 이해관계자는 보안사고 예방 및 안전한 업무환경 조성을 위해 상호 협력한다.

부 칙

1. (시행일) 본 정책은 2025년 11월 1일부터 시행한다.
2. (개정) 본 정책의 제정 및 개정은 소관 부서의 검토를 거쳐 시행한다.
3. (소관 부서) 본 정책의 소관 부서는 인사총무Part로 한다.