SJG아센텍 정보 보안규정

2026.02

문서 번호	2026-S-04
담당팀	총무팀
최초 제정일	2026. 02. 13
최근 개정일	-

1. 개요

1) 제정목적

본 규정은 SJG아센텍의 핵심기술보호와 정보보호 활동을 위한 기반 조직을 구성하고, 비인가자의 부적절한 행위로부터 당사 근무인원 및 시설을 안전하게 보호하는 것과 정보시스템에 의하여 처리, 저장, 소통되는 자료를 바이러스, 해킹 등의 위협으로부터 보호하고 취약 요인을 제거하여 회사의 핵심기술보호 및 정보보호 관리를 지속적으로 이루어지게 하는 것을 목적으로 한다.

2) 적용 범위

본 규정은 당사의 모든 조직과 임직원, 계약 관계에 있는 자, 출입자, 정보자산이 기록, 저장, 활용되는 모든 매체, 전산장비 및 관련시설을 포함한 모든 정보자산에 적용된다.

2. 선언

1) 역할과 책임

임직원 및 계약관계에 있는 모든 직원은 본 규정 및 관련 요령에서 정하는 보안정책을 준수해야 한다. 보안교육에 참석할 의무가 있고, 자체 점검 등 회사 보안활동에 적극 협조해야 한다. 영업비밀을 과도하게 취득, 보관하거나 사외로 무단 반출하는 등 보안사고의 개연성이 있는 행위를 해서는 안된다. 회사의 정보자산 반출 시 정해진 절차에 따라야 하며 임의 판단으로 반출할 수 없다. 출입증은 항상 패용해야 하며 출입증을 타인에 대여, 공유하지 않는다. 보안사고를 발견하였을 경우 팀 별 보안책임자 또는 보안담당조직에 즉각 해당사실을 알려야 한다.

회사의 보안규정을 위반하는 경우 다음과 같은 인원에 책임이 있다.

① 임직원이 보안규정 위반 : 위반자 및 소속 팀장
② 방문자가 보안규정 위반 : 방문 요청 또는 허가한 임직원

당사를 방문하는 방문자는 출입증을 소속회사의 직원이나, 타인에 대여, 공유하는 행위를 해서는 안된다. 카메라 또는 카메라폰과 같은 영상 기록장치를 이용한 임의촬영을 금지한다. 당사에서 제공된 자료 외 어떤 자료도 취득, 사용해서는 안 된다. 당사에서 요구하는 보호조치를 준수해야 하며 위반 시 사규와 관련 법령에 따른 모든 책임을 진다. 출입증을 대여하거나 본 목적과 다르게 사용하는 등 오남용 적발 시 해당자의 출입증 회수 및 출입 금지 조치하며, 소속사 대표이사에 재발방지 대책을 요구한다. 보호구역내에서는 당사의 통제를 따라야 하며, 이를 위반 시 강제 퇴실 또는 퇴장된다. 당사 자료를 무단으로 취득, 활용하거나 유출을 시도하는 경우는 사규와 관련 법령에 따른 민형사상 책임을 진다.

3. 보안 관리

1) 보안 위반자 관리

CSO(전사보안책임자)는 보안 업무를 총괄하는 본부장이 겸직하며, 해당 직위에 보임된 자가 CSO의 역할과 책임을 수행한다. CSO는 전사 보안정책의 수립·시행을 총괄하고, 보안 위반 사항에 대한 최종 의사결정 권한을 갖는다. 전사보안담당자는 위반사항의 경중을 판단하여, 경미한 위반의 경우 CSO명의의 주의조치를 해당 직원 및 소속 팀장에 통보하며, 중요한 위반이라고 판단되는 경우 CSO보고 후 규정에 따라 조치한다. 보안 위반에 대한 기준 및 징계는 내규에 의거하여 진행하고 범위를 벗어날 경우 징계관리규정에 정한 징계 종류 및 절차에 따른다. 유사사고 재발방지를 위한 대책을 수립, 시행하고, 징계 결과는 임직원 전원에게 공지할 수도 있다.

보안관리규정을 위반한 사실을 인지한 임직원은 전사보안책임자 또는 전사보안담당자에 즉시 위반 사실을 통보해야 한다. 본인의 실수 또는 의도하지 않게 정보가 노출, 제공되었음을 확인하는 경우 전사보안책임자 또는 전사보안담당자에 관련 사실을 통보해야 한다.

2) 보안 경중 판단 기준

[경미한 위반]

1) 위반 내용이 실수 또는 과실에 의한 단순한 규칙/지침 위반이라고 인정되는 경우
2) 위반이력이 없는 임직원이 규정, 절차 등의 미 인지로 규칙/지침을 위반한 경우
3) 본인의 위반사실을 통보해온 경우 중 중대한 위반에 사유가 되지 않는 경우

4) 위반회수에 따라 다음과 같이 조치를 상향한다

① 1회 위반: 당사자 구두 경고
② 2회 위반: 당사자 서면 경고(시말서) 및 팀장 구두경고
③ 3회 위반: 당사자 및 팀장 서면 경고(시말서)
④ 4회 이상: 고의적 정책 미 준수로 중대한 위반으로 상향

[중대한 위반]
인사징계위원회에 회부하여 경고 이상의 징계를 시행한다.
1) 고의로 보안 규정, 절차, 지침을 우회하는 행위를 한 경우
2) 보안사고와 직, 간접적으로 관련된 사안으로 인정되는 경우
3) 중대한 과실이거나, 동일한 위반을 반복적으로 지적 받는 경우

4. 영업비밀 관리

1) 영업비밀의 정의

'영업비밀'이란 비밀로 유지된 생산방법, 판매방법, 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말하며, 회사가 사용을 위하여 타사와의 계약관계 등을 통하여 도입한 타사의 영업비밀을 포함한다.

2) 영업비밀의 보관 및 관리

영업비밀은 생성시 원본 문서에 해당 등급을 표기해야 하며, 생성과정에 있는 중간산출물 및 해당내용의 일부를 사용한 문서도 동일한 방법으로 관리되어야 한다. 기 생성된 문서 중 보안등급이 구분되지 않는 문서의 경우 보안의 날에 등급 분류를 시행한다.

3) 출력된 영업비밀에는 그 등급이 매 페이지마다 쉽게 식별 가능하도록 표기되어야 하며, 출력 시 표기하지 못한 문서의 경우 출력 후 고무인 등을 활용하여 표기한다.

4) 출력된 영업비밀은 개방된 장소에 보관해서는 안되며, 시건 장치가 있는 장소에 보관하고 팀 보안책임자가 지정하는 자가 관리한다.

5) 출력된 영업비밀은 보존기간이 만료되면 1개월 이내에 복원할 수 없는 형태로 파기한다. 단, 업무적 이유로 파기를 유예할 필요가 있는 경우 목적과 유예기간 등을 서면으로 CSO에 보고 후 보관한다.

6) 영업비밀이 휴지통, 공용 회의실 등 직원이 통제할 수 없는 장소에 방치된 경우 문서의 출력자, 해당 팀장을 보안규정위반으로 조치한다.

7) 보직 변동으로 해당 영업비밀을 소유할 필요가 없는 경우 전보자는 '업무인수인계서' 에 취급 영업비밀의 인수인계 내용을 작성하고, 전자문서 및 출력문서 등 모든 종류의 영업비밀을 인수자에 인계한다.

8) 팀별 보안책임자는 인계/인수 절차에 따라 영업비밀이 적절히 이관되었는지 확인하고 인계자 소유하고 있는 영업비밀이 모두 파기되었는지 확인한다.

9) 업무상 이유로 기존 영업비밀의 일부를 전보된 팀에서 사용할 필요가 있는 경우 그 목적과 파일의 목록을 이전 팀 보안책임자에 서면으로 보고 후 활용할 수 있다. 서면보고과정 없이 보유하는 경우 이유를 막론하고 고의적인 정보취득으로 보안위반자 처리규정에 따라 조치한다.

10) 영업비밀을 본인의 업무와 직접적으로 관련이 없는 곳으로 반출할 사유가 발생하거나 국가기관 등 외부에서 요청한 자료의 범위에 영업비밀이 포함되는 경우 전사보안책임자의 사전 승인을 얻어 반출한다.

11) 본인의 업무 수행을 위해, 사외 반출하는 경우 반출처와 반출일시, 반출 내역을 회사가 정한 양식에 따라 작성하여, 주간 단위로 팀 보안책임자에 보고하고, 결재를 받아 보관한다. 단, 기술자료(도면)를 배포/접수할 수 있는 시스템이 구축된 경우 별도의 기록을 작성하지 않고 시스템 로그로 대체한다.

12) 영업비밀의 반출 이력은 2년 이상 보관되어야 하며, 필요 시 쉽게 조회 가능한 상태로 관리되어야 한다. 사내 배포의 경우 영업비밀의 소유권자(작성자)의 판단에 따라 회사가 정하는 보호조치가 적용된 상태로 필요한 인원에 한정하여 배포한다.

13) 본인이 작성한 영업비밀이 아닌 경우 배포, 반출할 수 없으며, 작성자의 승인을 얻거나 작성자에 반출, 재 배포를 요청해야 한다.

14) 전자문서 형태의 영업비밀은 회사가 정하는 방식으로 복원 불가한 상태로 파기해야 한다.

15) 전자문서 이외의 영업비밀은 문서세단기를 사용하여 원형을 확인할 수 없는 상태로 파기해야 한다. 임직원이 사용할 수 있는 문서세단기가 설치되지 않은 경우 전사보안담당자는

별도의 파기절차를 수립하여 운영해야 한다.

5. 부칙

- 본 정보 보안규정은 2026. 02. 13부로 제정한다.