Autonomous™

| 문서관리번호 | 2025-S-12 |
|---|---|
| 최종 수정일 | 2025. 6. 30 |
| 문서 관리자 | 기획팀 |

# ㈜오토기기 정보보안 정책

2025. 06. 30

# 1. 총칙

## 가. 제정 목적

본 정책은 현대자동차(이하 '당사'라 한다)의 유·무형의 영업비밀 및 경영활동 보호에 필요한 체계를 정의하고 지속적인 보호활동을 유지하여 정보보안 사고를 예방하고 당사 발전에 기여함을 목적으로 한다.

## 나. 적용 범위

본 정책은 당사의 임직원 및 외부자, 당사를 출입하는 모든 인원을 대상으로 적용하며 당사가 보유 및 운영하고 있는 모든 정보자산에 적용한다.

# 2. 정보보안 준수 의무

## 가. 정보보안 준수 의무

① 당사는 정보보안 관리 시스템을 지속적으로 점검하고 개선하기 위해 노력할 책임이 있으며, 모든 임직원은 당사의 보안 정책을 숙지하고 신의성실의 원칙에 따라 정책을 준수하여야 한다.

② 업무상 취득한 당사 또는 제3자 소유의 정보를 업무 목적 이외의 용도로 사용하거나 당사의 보안 정책에 따라 접근이 허용된 인원 외의 임직원 및 외부자에게 승인 없이 공개, 누설해서는 안 된다.

③ 임직원 및 외부자는 당사 정보자산을 안전하게 사용하고 정보보안 사고를 인지한 경우 전사 정보보안 담당조직에 즉시 알려야 한다.

④ 보안 관련 규정, 지침, 절차에 따라 모든 정보보안 업무를 처리하며 이에 명시되지 않은 사항은 관련 법령 및 사규가 정하는 바에 따라야 한다.

## 3. 외부 협업 보안

### 가. 계약 및 서약

① 당사와 업무 협업을 진행하는 경우 사전에 외부자를 대상으로 비밀유지를 위한 보안계약서 및 서약서를 징구하여야 한다.

② 외부자와 업무상 협업을 위한 계약을 체결하는 경우에는 당사 정보자산 보호에 필요한 사항을 검토하여 외부자가 준수해야 하는 사항을 계약서에 명시하여야 한다.

③ 계약 업무 수행 상 당사의 보안문서를 취급, 열람하는 외부업체의 인원 범위는 필요한 최소인원으로 한정해야 한다.

### 나. 외부 협업 보안관리

① 외부업체 직원은 당사에서 허가한 지역에 제한적으로 출입할 수 있고 업무 협업을 위해 전산장비를 반입하는 경우 당사의 전산장비 반출입절차를 준수하여야 한다.

② 외부업체 직원은 당사 보안 정책을 준수하고 정보보안 교육에 참석하여야 한다.

### 다. 협업 주관부서

① 협업 주관부서는 보안준수 사항을 주기적으로 교육하고 이행 여부를 점검하여야 한다.

## 4. 정보보안 사고 대응 및 예방

### 가. 정보보안 사고 인지 및 보고 절차

① 모든 임직원은 비인가된 활동을 인지하거나 이상징후를 발견하는 경우 내부 신고처, 사업장 부문보안관리자, 부서보안책임자에게 신고하여야 한다.

② 모든 임직원은 자의적인 판단에 의해 전사보안책임자의 사전 승인 없이 사고 조사와 무관한 임직원 및 당사 외부(언론사 포함)에 정보보안사고와 관련된 내용 일체를 누설해서는 아니 된다.

③ 보안담당자는 시스템에 비인가된 활동이나 이상징후가 보이면, 확인 및 점검 후 정보보안사고로 판단될 시 전사보안책임자에게 보고하여야 한다.

④ 침해사고 대응 및 원인분석, 사고조사를 수행하여 전사보안책임자에게 보고하여야 한다.

### 나. 복구 절차 및 사후 조치

① 시스템 담당자는 중요 파일을 백업하고 관련 시스템의 계정 정보를 변경하며, 시스템 복구 시 백업 이미지의 훼손/침해 여부를 검증하여야 한다.

② 복구된 시스템은 침해사고 취약점 제거 여부를 확인하고, 사고 발생 관련 최신 보안 패치 적용을 지원하여야 한다.

③ 보안 담당자는 피해 사실과 원인, 재발 방지 대책 등을 포함한 보고서를 작성하여 전사보안책임자에게 보고한다.

④ 사후조치로 사고 재발 방지를 위한 대응책을 마련한다.

### 다. 정보보안 사고 예방

① 정보보안 사고를 예방하기 위해 이상징후 모니터링 및 탐지·대응 체계를 구축하여 운영하고 정보보안 사고 대응 모의훈련을 정기적으로 실시한다.

② 침해사고 발생 시 신속한 대응을 위해 연1회 이상 침해사고 대응 모의훈련을 계획하고 실시하여야 한다.

## 5. 데이터 무결성 및 보호

### 가. 데이터베이스 보안

① 당사는 데이터베이스의 데이터 무결성 확보를 위하여 사용자가 직접 접근할 수 없도록 통제하여야 한다.

② 정상적인 인증방법 외의 방법을 통한 데이터베이스 데이터 수정을 금지하며, 수정 필요시, 데이터베이스 운영 담당자의 승인하에 인가된 인원에 한하여 수정이 가능하다.

③ 데이터베이스간 또는 데이터파일 공유는 원칙적으로 금지하며, 반드시 필요한 경우 보안성 검토 등 적절한 보안대책을 적용하여야 한다.

### 나. 보안시스템 로그 관리

① 당사는 보안시스템 로그가 위·변조되지 않도록 관리적, 기술적 보호 조치를 취하여야 한다.

② 중요 로그는 제3의 장소에 백업하고 안전하게 관리하여야 한다.

본 방침은 2025년 6월 30일부터 시행됩니다.