



동아특수화학(주)

## 정보보안 내부 규정

승인자	서무 이한경 차장
제정	2025년 12월 19일
개정	최초 제정
문서 관리 번호	DGP-0210
문서 관리자	서무 이한경 차장



## 제 1 장 [총 칙]

### 가. 목적

본 규정은 동아특수화학(주)의 정보 자산을 안전하게 보호하고, 정보 유출, 훼손, 변조 및 오용을 방지하여 회사의 경영 활동을 안정적으로 지원하며, 관련 법규 미 규제 준수를 목적으로 한다. 모든 임직원 및 회사의 정보 자산에 접근하는 모든 제 3 자에게 적용된다.

### 나. 적용 범위

본 규정은 회사의 모든 임직원(정규직, 계약직, 파견직 등), 협력업체 직원, 자문위원 등 회사의 정보 자산에 접근하거나 정보 시스템을 사용하는 모든 사람에게 적용된다. 또한, 회사의 모든 유무형 정보 자산(문서, 데이터, 시스템, 네트워크, 설비 등)에 적용된다.

### 다. 정보보안 원칙

회사는 다음의 정보보안 원칙을 준수한다.

#### 1. 기밀성 (Confidentiality)

인가된 사용자만이 정보 자산에 접근할 수 있도록 한다.

#### 2. 무결성 (Integrity)

정보 자산이 정확하고 완전하며, 인가되지 않은 변경으로부터 보호되도록 한다.

#### 3. 가용성 (Availability)

인가된 사용자가 필요할 때 정보 자산을 사용할 수 있도록 한다.

## 제 2 장 [정보보안 조직 및 책임]

### 가. 정보보안 책임자

정보보안 책임자는 회사의 정보보안 정책 수립, 이행 감독, 정보보안 활동 총괄 등 전반적인 정보보안 업무를 책임진다.

### 나. 정보보안 담당 부서

정보보안 담당 부서는 정보보안 책임자의 지휘 아래 정보보안 정책의 실행, 보안 시스템 운영 및 관리, 보안 교육 및 인식 제고 활동 등을 수행한다.

### 다. 모든 임직원의 책임

모든 임직원은 본 규정을 숙지하고 준수할 의무가 있으며, 할당된 정보보안 책임을 성실히 이행해야 한다.



## 제 3장 [정보 자산 분류 및 관리]

### 가. 정보 자산 분류

회사의 모든 정보 자산은 중요도 및 민감도에 따라 다음과 같이 분류된다.

#### 1. 대외비

외부에 공개될 경우 회사에 심각한 손해를 초래할 수 있는 정보 (예: 핵심 기술 자료, 미공개 재무 정보, 주요 계약 정보).

#### 2. 회사 기밀

회사 내부에서만 공유되어야 하며, 외부 유출 시 회사에 손해를 줄 수 있는 정보 (예: 인사 정보, 고객 정보, 내부 회의록)

#### 3. 일반 정보

외부에 공개되어도 회사에 큰 영향을 미치지 않는 정보 (예: 일반 업무 자료, 공개된 홍보 자료).

### 나. 정보 자산 관리

1. 분류된 정보 자산은 해당 등급에 맞는 보안 수준으로 관리되어야 한다.

2. 정보 자산의 생성, 저장, 전송, 폐기 등 전 생명주기에 걸쳐 보안 보치가 적용되어야 한다.

## 제 4장 [접근 통제 정책]

### 가. 사용자 계정 관리

1. 모든 정보 시스템 접근은 인가된 사용자 계정을 통해서만 가능하다.

2. 계정은 개인별로 부여하며, 타인과 공유하는 것을 금지한다.

3. 비밀번호는 정기적으로 변경하고, 복잡성 규칙을 준수해야 한다.

### 나. 시스템 및 정보 접근 권한

1. 사용자는 자신의 업무 수행에 필요한 최소한의 정보 및 시스템에만 접근 권한을 부여받는다.

2. 접근 권한은 정기적으로 검토하고, 직무 변경 또는 퇴사 시 즉시 회수되어야 한다.

### 다. 원격 접근

1. 원격 접근은 반드시 회사가 승인 보안 채널(VPN 등)을 통해서만 가능하며, 보안 지침을 준수해야 한다.

## 제 5장 [시스템 및 네트워크 보안 정책]



#### 가. 시스템 보안

1. 모든 시스템(서버, PC, 모바일 기기 등)은 최신 보안 패치가 적용되어야 한다.
2. 백신 소프트웨어를 설치하고 항상 최신 버전으로 유지하며, 실시간 감시 기능을 활성화해야 한다.
3. 불법 소프트웨어 설치 및 사용을 금지한다.

#### 나. 네트워크 보안

1. 네트워크 장비는 적절한 보안 설정이 적용되어야 한다.
2. 방화벽, 침입탐지/방지 시스템 등 보안 시스템을 운영하여 외부 침입 및 내부 정보 유출을 방지한다.
3. 무선 네트워크(Wi-Fi) 사용 시 보안 설정(암호화 등)을 강화한다.

#### 다. 데이터 백업 및 복구

1. 중요 정보 자산은 정기적으로 백업하고, 백업된 데이터는 안전하게 보관한다.
2. 재해 발생 시 신속한 복구를 위한 절차를 수립하고 주기적으로 점검한다.

### 제 6 장 [물리적 보안 정책]

#### 가. 출입 통제

1. 서버실, 중요 문서 보관실 등 주요 정보 자산이 보관된 구역은 출입 통제 시스템을 운영한다.
2. 인가되지 않은 자의 출입을 엄격히 제한하고, 출입 기록을 유지한다.

#### 나. 자산 보호

1. 모든 정보 자산은 도난, 훼손, 화재 등으로부터 보호될 수 있도록 관리한다.
2. 사용하지 않는 PC, 노트북 등은 잠금장치를 사용하고, 중요 문서나 저장매체는 잠금 가능한 장소에 보관한다.

### 제 7 장 [정보보안 교육 및 인식 제고]

#### 가. 정보보안 교육

1. 모든 임직원은 정보보안 의식을 높이고 본 규정을 이해할 수 있도록 정기적인 정보보안 교육을 이수해야 한다.
2. 신규 입사자는 입사 시 정보보안 교육을 필수적으로 이수해야 한다.

#### 나. 보안 인식 제고 활동

1. 정보보안 관련 최신 위협 정보 및 보안 수칙을 주기적으로 공유하여 임직원의 보안 인식을 강화한다.



## 제 8 장 [정보보안 사고 대응 및 복구]

### 가. 사고 신고 및 처리

1. 정보보안 사고(정보 유출, 시스템 침해, 악성코드 감염 등) 발생 시 즉시 정보보안 담당 부서에 신고해야 한다.
2. 신고된 사고는 사고 대응 절차에 따라 신속하게 조사하고 조치한다.

### 나. 복구 및 재발 방지

1. 사고로 인한 피해를 최소화하고 시스템을 정상 상태로 복구한다.
2. 사고 원인을 분석하여 재발 방지 대책을 수립하고 이행한다.

## 제 9 장 [법규 준수 및 감사]

### 가. 법규 준수

회사는 정보보안 관련 국내외 법규 및 규제(개인정보보호법, 정보통신망법 등)를 준수한다.

## 제 10 장 [규정 위반 시 조치]

본 규정을 위반한 임직원은 회사의 인사 규정 및 관련 법규에 따라 징계 또는 법적 조치를 받을 수 있다.

## 제 11 장 [규정의 제정 및 개정]

본 규정은 [제정일]부터 시행하며, 정보보안 환경 변화 및 관련 법규 개정에 따라 필요시 개정될 수 있다.



2025. 12. 19

동아특수화학주식회사 대표이사 전병길

