그룹 정보보호 정책

정보보호 경영방침

제정: 2024.05.28

우리 COSMAX 그룹은 화장품 및 바이오 분야의 선도적 ODM 및 OBM 기업으로서, 회사의 가치를 높이고 고객에게 최상의 서비스를 제공하기 위해 정보보호 활동은 선택이 아닌 필수 불가결한 요소가 되었습니다.

따라서, COSMAX 그룹의 모든 임직원은 내부 및 외부의 신뢰 구축과 사회적인 책임을 다하기 위해 정보보호 및 개인정보 보호와 관련된 법규와 이해 관계자들의 정보보호 요구사항들을 준수해야 합니다.

또한, COSMAX 그룹의 핵심 기술 및 인력들의 유출, 내부 및 외부로부터의 각종 침해사고 등 수많은 정보보호 위협으로부터 중요 정보자산을 보호하기 위한 대비책을 마련하는데 최선을 다해야 합니다.

COSMAX 그룹 정보보호 정책

제 1 장 목적

그룹 정보보호 정책 (이하 "정책"이라고 함)은 COSMAX 그룹 내 계열사, 국내 및 국외 관계사(이하 '회사'라고 함)들이 비즈니스 활동을 수행하는데 필요한 정보보호, 개인정보보호, 이해 관계자들과의 계약 등의 제반 법규 요구사항들(이하 '컴플라이언스'라고 함)을 준수하고 이와 관련하여 사용 또는 관리하고 있는 정보자산들을 안전하게 보호하기 위하여, 글로벌 ONE COSMAX 정보보호 관리체계 수립에 관한 원칙을 정하는 데에 그 목적을 둔다.

회사는 본 정책에 기반하여 이를 대상회사의 사업 영역 관련 제반 컴플라이언스 준수에 필요한 요구 사항, 사업 및 정보보호 운영 환경과 위험 등을 고려하여 이를 효과적으로 이행할 수 있도록 세부 정보보호 규정 및 지침 등을 제정하고 시행해야 한다.

제 2 장 적용 범위

본 정책은, 회사 전체와 회사에 근무하는 전 임직원을 대상으로 하며, 회사의 협력회사 직원, 일용 근로자 등 계약관계에 있는 특수인 및 회사 정보자산에 접근이 필요한 제3자에게도 적용한다. 또한 회사의 정보자산 및 회사가 위탁 받은 정보자산에도 적용된다.

정보보호 관련 국내/국제법이나 정부 정책은 본 정책보다 우선하여 적용된다.

제 3 장 정의

1.1. 정보보호 관련 규정의 체계와 본 정책의 위치

정보보호 상의 위험은 경영활동의 수행과 정보기술의 발전과 동반하여 항상 변화하고 있다. COSMAX 그룹의 정보자산을 적절하게 보호하기 위해서는 회사 현황의 변화나 새로운 위협의 발생 등에 대해 정보보호 대책을 정기적으로 점검할 필요가 있다. 이에 따라 회사는 「COSMAX 그룹 정보보호 정책」을 정보보호 상위 규정으로서 정하고 환경변화에 맞춰 정기적인 점검이 필요한 「정보보호 규정, 지침 및 각종 절차서」들을 하위 규정으로 정하는 것으로 한다. 단, 정보보호 관련 국내/국제법이나 정부 정책은 본 정책이나 회사별 규정 및 지침보다 우선하여 적용된다.

(1) COSMAX 그룹 정보보호 정책
- COSMAX 그룹의 정보보호 최상위 규정으로서, COSMAX 그룹의 정보보호 관리체계 및 정보보호 수준을 통일하고 향상시키기 위한 원칙을 정한 정책

(2) 회사별 정보보호 규정
- 본 정책을 근거로 각 회사별 특수성을 고려한 컴플라이언스 준수와 정보보호 요구사항들의 이행에 필요한 정보보호 관리체계 구축과 그 운영에 필요한 원칙들을 정한 규정

(3) 그 외, 하위규정
- 기준에 근거하여 각 회사별 특정한 범위 내에서 준수해야 할 정보보호 관련 세부 절차나 수행 방법 등을 더욱 구체적으로 정한 지침, 절차서 또는 가이드와 같은 정보보호 관련 규정 류

1.2. 용어의 정의

본 규정에서 사용하는 용어의 정의는 다음과 같다.

(1) 정보: 정보는 업무상 취급하는 문서나 도면, 전자기록, 업무를 통해 알게 된 지식 등,

유형무형을 가리지 않고, 모든 형태의 것을 말한다.

(2) 정보시스템: 하드웨어, 소프트웨어, 네트워크 등으로 구성되어, 정보를 처리하는 것을 말한다. 각각의 구성요소를 가리키는 경우도 있다.

(3) 정보자산: 정보 및 정보를 처리하는 정보시스템을 총칭한다.

(4) 위협: 정보자산에 대해 손해를 가하는 잠재적인 요인을 말한다.

(5) 사이버 공격: 위협의 일종으로 악의를 갖고 공격자가 정보시스템을 이용하여 부정하게 데이터를 조작하거나 프로그램을 실행하는 것을 말한다.

(6) 정보보호: 정보자산을 모든 위협으로부터 보호하고, 기밀성, 무결성 및 가용성을 확보하고 유지하는 것을 말한다.

(7) 정보보호 사고: 고의적 또는 사용자의 과실에 의해 회사 정보자산이 유출, 조작되는 등의 사건, 사고를 말한다.

(8) 사용자 등: 회사의 정보자산을 이용하여 회사의 지시에 따라 업무를 수행하는 아래의 자를 말한다.

- 경영자 등 (대표, 임원, 고문 등)
- 임직원 (회사의 사원, 계약사원, 임시고용자, 단기근로자를 포함하며 회사와 고용 관계에 있는 자)
- 파견계약에 따른 파견직원
- 기타 대상 회사와의 프로젝트나 위탁업무 계약 등을 통해 회사의 정보자산에 접근이 필요한 제3자

제 4 장 정보보호의 책임

1.1. 정보보호 최고책임자(CISO: Chief Information Security Officer)

회사의 정보보호 활동에 대한 총괄 및 정보보호 조직을 운영하는 책임을 가지며, 정보보호의 방향과 정보보호관리체계 운영의 일관성을 지속적으로 유지해야 하는 책임이 있다.

1.2. 정보보호 주관부서

회사 정보보호에 대한 기획, 조정, 지원 등의 업무를 수행하며, 정보보호 규정 및 지침의 제정 및 개정, 정보보호 관련 법규 및 이해 관계자들의 정보보호 요구사항 등의 대응할 책임이 있으며, 주기적으로 정보보호 규정 및 지침의 준수여부 및 적용된 정보보호 대책의 적합성을 검토하고, 이를 정보보호 최고책임자에게 보고할 책임을 갖는다.

1.3. 사용자 등은 본인에게 허락된 정보자산만을 이용 및 관리해야 할 책임이 있다.

회사는 본 정책에 기반하여 이를 대상회사의 사업 영역 관련 제반 컴플라이언스 준수에 필요한 요구 사항, 사업 및 정보보호 운영 환경과 위험 등을 고려하여 이를 효과적으로 이행할 수

있도록 세부 정보보호 규정 및 지침 등을 제정하고 시행해야 한다.

제 5 장 정보보호 행동지침

회사는 정보보호 관련 규정에 근거하여 글로벌 수준의 정보보호 관리체계를 적절하게 운영하고 지속적으로 유지 및 수준 향상을 위해 노력해야 한다. 이를 실현하기 위해 회사는 다음의 항목을 실시한다.

(1) 정보보호 관리체계의 구축
(2) 정보보호 관리 프로세스의 명확화
(3) 정보자산이 갖고 있는 위험 식별 및 평가
(4) 정보보호 대책의 책정

또한, 사용자 등은 이러한 대처의 필요성을 이해하고, 자신이 취급하는 정보자산에 대해 다음과 같은 항목을 실천한다.

(1) 업무상 필요한 자에게만 정보를 공개한다.
(2) 정해진 정보자산의 취급 규칙에 따라 업무를 수행한다.
(3) 정보보호에 관한 교육 및 연수에 참여한다.
(4) 정보보호 대책 미비, 기밀정보 누설, 조작 등을 알게 된 경우, 정해진 절차에 따라 신속하게 보고한다.

제 6 장 정보보호 기본원칙

1.1. 정보자산의 취급

사용자 등은 회사의 정보자산이 유출, 조작되는 등의 정보보호 위험으로부터 보호하기 위해 다음과 같은 항목을 실시해야 한다.

(1) 정보
- 정보는 용도 및 목적에 따라 분류해야 한다.
- 분류된 정보는 기밀성에 따라 정보의 중요도를 평가하고, 평가된 중요도에 따라 적절한 정보보호 대책을 수립하여 실시해야 한다.
- 정보는 분류 등급을 표기해야 한다.
- 정보는 정보의 생명주기(생성, 이용, 저장, 폐기)에 따라 정보보호 대책을 수립하여 실시해야 한다.

(2) 정보시스템

- 정보시스템은 용도 및 목적에 따라 분류해야 한다.
- 분류된 정보시스템은 기밀성, 무결성, 가용성에 따라 중요도를 평가하고, 평가된 중요도에 따라 적절한 정보보호 대책을 수립하여 실시해야 한다.
- 정보시스템은 기획, 개발, 운용, 보호, 폐기 등의 생명주기에 따라 정보보호 대책을 수립하여 실시해야 한다.

1.2. 인적 보안

회사는 임직원 등의 채용, 이동, 퇴직 등 정보자산의 사용자가 추가 또는 변경이 발생한 경우 정보보호 관리체계에 대한 준수의무를 부과하기 위해 비밀유지에 대한 계약을 별도로 체결하는 등 인적 보안 대책을 수립하고 실시해야 한다. 또한, 정보보호의 중요성을 사용자 등이 이해하고, 정보자산을 적절하게 취급할 수 있도록 정기적으로 정보보호에 관한 교육을 실시해야 한다.

1.3. 물리적 보안

회사는 재해 또는 범죄 등의 물리적인 위협으로부터 회사의 정보자산을 안전하게 보호하기 위해 사무실이나 사업장 내 출입, 정보자산이 보관 및 설치된 장소에 대한 출입 등에 대해 적절한 물리적 보안대책을 수립하고 실시해야 한다.

1.4. 기술적 보안

회사는 사이버 공격 등의 다양한 위협으로부터 회사의 정보자산을 보호하기 위해, 접근 제어, 정보의 암호화, 바이러스 대책 등 기술적인 보안 대책을 실시해야 한다.

1.5. 정보보호에 대한 외부위탁

회사는 정보자산을 이용하는 업무를 외부 위탁하는 경우, 정보보호 요구사항이 명시된 계약을 체결하는 등 외부위탁과 관련하여 적절한 정보보호 대책을 수립하고 실시해야 한다.

1.6. 개인정보 보호조치

회사는 비즈니스 목적에 의해서만 사용자 등 및 제3자의 정보를 필요한 범위 안에서 최소한으로 수집, 보관 및 처리해야 한다.

1.7. 정보보호 사고에 대한 대책

회사는 정보보호 사고가 발생할 경우를 대비하여, 피해를 최소화하기 위한 대응 절차를 수립하고 정비해야 한다.

1.8. 피해 시의 정보보호 확보

회사는 대규모 재해나 정보시스템의 장애발생 등, 비즈니스의 연속성을 위협하는 위험이 발생하는 경우를 가정하여 복구 및 재개를 위한 절차를 수립 또는 정비할 때, 정보보호에 대한 유지도 고려해야 한다.

1.9. 정보보호 점검 혹은 감사

회사는 정보보호 대책의 유효성을 평가하기 위해, 정보보호 관련 규정의 준수 현황을 정기적으로 확인하고 결과에 따른 정보보호 대책을 재검토해야 한다. COSMAX 그룹은 소속된 회사들에 대한 정보보호 관리체계의 지속적인 운영 및 개선활동 등의 이행 여부를 확인하고 결과에 따른 정보보호 대책을 회사들에게 권고해야 한다.

제 7 장 정보보호 컴플라이언스 준수

사용자 등은 사회적인 책임을 다하기 위해 본 정책 또는 관련된 법령을 준수하는 것은 물론, 본 정책에 기재되지 않은 법령, 사내 규정을 준수해야 한다.

제 8 장 위반에 대한 조치

회사는 사용자 등이 본 정책이나 각 회사별 하위 규정에서 정한 사항들을 위반한 경우, 취업규칙, 인사규정 및 개별계약 등에 근거하여 조치를 취해야 한다.

제 9 장 예외 조치

COSMAX 그룹은 합리적 사유가 있는 경우에 한하여 정보보호 관련 규정의 예외조치를 인정한다. 합리적인 사유란 본 정책의 적용이 지역의 특성이나 법령에 맞지 않거나, 적정한 업무 수행에 현저하게 방해가 되는 경우 등을 말하며, 회사는 예외조치에 대처하기 위한 절차를 마련해야 한다.

제 10 장 정보보호 관련규정의 검토 및 개정

회사는 정기적으로 정보보호 관련 규정의 검토를 수행해야 하며, 새로운 위협의 출현 등에 따라 위험이 변화하는 경우에도 적시에 검토를 수행해야 한다. 정보보호 관련 규정을 개정하게 되는

경우에는 회사별 내부 규칙에 따른다.

부 칙

이 정책은 2024년 5월 28일부터 시행한다.

1. 제정 2024년 5월 28일