현대그린푸드

정보보호 정책

HYUNDAI
GREEN FOOD

현대그린푸드는 정보보호 관리체계 수립, 구축, 운영 및 개선에 필요한 기본 사항을 규정하여 정보보호 활동의 범위와 기준을 제시하고 안전한 서비스를 제공하기 위한 정보보호 관리체계 기준을 수립 및 운영하고 있습니다.

정보보호 정책은 세부 지침, 가이드로 구성되며 임직원 및 본 정책의 범위 내에서의 시간제 근로자, 협력업체, 방문자, 기타 회사와 계약관계에 있는 자, 그리고 회사를 출입하는 모든 인원에게 적용됩니다.

1. 정보보호 정책 수립 및 운영

현대그린푸드는 위험관리를 통해 전반적인 보안운영에 대한 일관성 유지를 위해 임직원 및 협력업체 등 현대그린푸드 정보자산에 접근 권한을 가지는 모든 인력들이 준수해야 할 정보보호 정책, 지침, 가이드를 구성하여 운영합니다.

정보보호 정책에 기본 원칙을 정의하고, 해당 원칙을 이행하기 위해 상세 행동명령을 정의한 정보보호 지침 및 가이드를 운영하며 전 임직원 및 사내 정보자산 및 시스템에 접근 권한을 가지는 모든 인력을 대상으로 정책이 적용됩니다. 외부환경(법령, 규제, 상위 조직의 정책 등) 및 정보보호 관리체계의 변화에 따른 요구사항을 주기적으로 검토하여 연 1 회 이상 개정합니다.

2. 정보보호 조직

현대그린푸드는 정보보호 정책에 규정된 정보보호 활동을 효율적으로 수행하기 위해 정보보호 최고책임자를 지정하고 정보보호 전담 조직을 구성하여 운영합니다.

정보보호 및 개인정보보호 업무를 전담으로 맡고 있는 보안조직을 구성하고 있으며 정보보호 최고책임자 주관하에 정보보호 및 개인정보보호의 주요 사안에 대한 검토 및 의결을 위해 정보보호 위원회를 주기적으로 운영합니다.

3. 정보자산 관리

현대그린푸드는 보호해야 할 정보보호 관리체계 범위의 정보자산을 식별하고 정의된 기준에 따라 식별한 정보자산이 안전하게 보호될 수 있도록 관리합니다.

식별된 정보자산에 대해 항상 최신 목록으로 관리하고 있으며 각 정보자산에 보안등급 부여 및 보안등급에 따른 보호대책을 적용하고 비인가 접근, 유출, 위/변조 등의 보안위협으로부터 보호합니다.

4. 정보보호 관리체계

현대그린푸드는 정보보호 정책과 지침을 기반으로 한 정보보호 관리체계 운영을 통해 개인정보를 포함한 중요 정보자산이 안전하게 보호될 수 있도록 관리합니다.

연 1 회 이상 정보보호 관리체계 점검을 실시하여 안전한 사업의 영위를 위해 준수해야 하는 법적, 제도적 요구사항에 대한 준수 여부를 확인하고 점검 결과를 통해 정보보호 관리체계 개선방안을 수립 및 이행합니다.

5. 물리적 보안

현대그린푸드는 임직원이 근무하는 본사와 데이터센터를 포함한 회사가 운영하는 사업소/센터/사업장에 대해 안전한 근무환경을 유지하고 시설 내 정보자산을 보호하기 위한 물리적 보안 지침을 수립하여 운영합니다.

발생 가능한 보안 위험(정보 및 정보자산 훼손, 변조, 도난, 유출 등)을 식별하고 물리적 통제가 필요한 지역을 중요도에 따라 각각의 보호구역으로 설정하여 구역별 보호대책을 수립 및 이행합니다.

6. 인적 보안

현대그린푸드는 내부 임직원과 외부자 등에 의해 발생 가능한 보안 위험을 식별하고 보안 위험을 제거하기 위해 필요한 보호대책을 수립 및 이행합니다.

임직원들이 준수해야할 사항들에 대해 서약서 징구 및 관련 교육을 실시하여 구성원으로서의 의무와 책임을 다하도록 관리합니다.

7. 정보시스템 보안

현대그린푸드는 회사의 모든 정보자산을 보호하고 안전한 서비스를 제공하기 위해 모든 형태의 정보시스템에 대해 정보보호 관리체계를 수립하여 운영하고 점검합니다.

모든 형태의 정보시스템에 대해 도입, 변경 및 운영 시 발생 가능한 보안 위험을 식별하고 제거하기 위해 주기적으로 모의해킹, 취약점 진단 등을 통해 서비스 및 중요 데이터를 보호합니다.

8. 사업연속성 관리

현대그린푸드는 재해와 보안사고 등으로 회사의 중요 서비스가 중단되지 않도록 필요한 절차와 대응 체계를 수립 및 이행하여 사업연속성을 보장합니다.

재해복구 계획의 효과를 보장하기 위해 정기적으로 모의훈련을 실시하고 훈련 결과 분석을 통해 재해복구 계획을 개선하고 지속 관리합니다.