정보보호 규정

총 칙

제1조 (목적)

본 규정은 ㈜드림어스컴퍼니(이하 "회사"라 함)의 정보보호 활동 위해 필요한 사항을 규정하여 회사의 정보자산을 보호함에 목적이 있다.

제2조 (적용범위)

본 규정은 회사가 보유하고 있는 모든 정보자산을 대상으로 하며, 전 임직원 및 회사의 업무에 종사하는 관계사 직원, 아웃소싱 인력, 임시직원 등을 포함하는 외부인력에게 적용한다.

제3조 (책임과 역할)

① 정보시스템을 통하여 생산, 저장, 전송, 처리되는 정보와 이에 의하여 제공되는 정보서비스는 회사의 중요한 자산이다.
② 회사의 정보자산은 그 가치와 중요성에 적합한 수준으로 자연재해, 시스템 및 네트워크의 고장, 내·외부 인원에 의한 우발적이거나 의도적인 각종의 위협으로부터 보호되어야 한다.
③ 회사의 모든 임직원, 외부업체 직원은 본 규정을 이해하고 준수함으로써 회사의 정보자산을 보호할 책임이 있다.

제4조 (정보보호 대상)

① 정보보호의 대상은 회사의 정보자산으로 한다. 정보자산은 정보와 정보시스템으로 구분되며, 이를 운영하기 위하여 필요한 정보 관련 자산 역시 정보보호의 대상이 된다.
② 정보는 회사 임직원들이 경영활동과 관련하여 생성 또는 입수하여 소유하고 있는 지적 자산 등 컴퓨터나 저장매체에 기록된 정보와 각종 인쇄물 등을 포함한다.
③ 정보시스템은 회사가 사용 또는 관리하는 모든 하드웨어, 소프트웨어, 네트워크 등을 포함한다.
④ 정보 관련 자산은 정보 및 정보시스템에 관련된 인력, 시설, 장비 및 운영을 위한 규정 및 절차 등을 포함한다.

제5조 (정보보호 요구사항)

회사의 정보자산은 다음과 같은 요구사항을 충족하여야 한다.

1. 기밀성 : 정보가 권한이 없는 사람에게 공개되지 않아야 한다
2. 무결성 : 정보가 권한이 없는 사람에 의해 변경되지 않고, 정확하고 완전한 상태로 유지되어야 한다
3. 가용성 : 권한이 있는 사람이 정보에 대한 접근을 필요로 할 때, 적정한 시간 내에 이용 가능해야 한다
4. 준법성 : 회사의 정보보호 관련 법적인 요구사항을 준수하여야 한다

정보자산 관리

제6조 (정보자산의 식별 및 관리)

① 회사의 모든 정보자산은 식별되고, 식별된 정보자산에 대해서 목록을 작성하여 이를 주기적으로 검토, 변경해야 한다.

② 정보자산이 인사이동(퇴직, 전보 등) 및 신규로 발생되는 경우 정보자산 소유자는 정보보호 담당자에게 통보하고 부서 내 관리하는 정보자산목록에 등록해야 한다.

③ 식별된 정보자산에 대한 실제 관리·운영하는 관리자 또는 담당자를 지정하여 책임소재를 명확하게 하여야 한다.

④ 정보자산의 등급은 정보를 최초 생성하는 정보의 소유자와 정보보호담당자가 정보의 중요도에 따른 적절한 수준의 보호를 하기 위하여 정보의 등급을 결정하고 그에 따른 보호 방법을 명시해야 한다.

제7조 (중요 정보의 분리)

① 회사의 정보자산을 중요도에 따라 구분하여 정보자산의 생성, 이용, 저장, 폐기 등의 처리 단계에 따라 비인가자에 의한 유출 및 변조 등을 방지할 수 있도록 관리 기준을 수립하고 운영함에 그 목적이 있다. 회사의 중요정보는 기본적으로 '대외비', '기밀'로 구분한다.

② 대외비란, 회사 내부의 경영정보에 관한 내용을 포함하여, 사외 공개가 금지된 정보이다. 이 정보에 대한 접근 권한은 회사 임직원만 취급할 수 있고 외부에 배포 시 문제를 야기하거나 손실을 가져와 반출을 억제해야 하는 정보이다.

③ 기밀정보란, 회사의 핵심적인 경영정보를 포함하여 고도의 보안이 요구되는 정보로서, 이 정보에 대한 접근 권한은 "업무상 알 권한이 있는 한정된 임직원"에게만 제공되도록 관리되어야 하는 정보이다.

제8조 (정보자산 등급 분류 및 표시)

① 회사의 정보자산에 대한 중요도를 평가하여 보안 등급별로 분류하고 정기적으로 적정성을 검토하여야 한다.
② 문서, 저장매체 등에는 회사 기준에 따라 보안 등급을 표시하고 관리하여야 한다.

제9조 (정보자산 등급별 관리)

① 정보자산은 보안 등급에 따라 취급절차(생성, 저장, 이용, 파기 등)수립 및 사용자를 지정하고 비 인가자의 접근을 차단하여야 한다.
② 중요 정보자산에 대해서는 주기적으로 보안점검 및 분석을 수행하고 발견된 취약점에 대해서는 통제대책을 강구하여야 한다.
③ 중요 자료 및 문서 등의 폐기시에는 해당 내용을 복구할 수 없도록 파기 또는 완전 삭제 등을 시행하여야 한다.

제10조 (위험관리)

① 정보보호 담당자는 정보자산의 취약·위협을 식별하고 발생빈도를 분석하여 위험을 도출하고, 이에 따른 효과적인 보호대책 수립을 위해서 위험분석 및 평가를 수행하여야 한다.
② 위험분석 및 평가를 위해, 필요 시 외부 전문가의 지원을 받을 수 있다.
③ 위험분석 및 평가로부터 도출된 위험에 대해서는 보호대책을 수립하여 적용함으로써 위험을 관리하여야 한다.

물리적 보안

제11조 (보호구역의 구분)

① 정보보호 담당자는 회사 내 정보보호 상 제한과 통제가 요구되는 지역(시설)은 보호구역으로 설정하며, 중요도에 따라 "통제구역", "제한구역", "일반구역"으로 구분·적용하여 관리하여야 한다.
② 기타 보호구역의 세부적인 사항에 관하여는 '물리보안 지침'에 따른다.

제12조 (보호구역 접근통제)

보호구역에 대한 출입 및 감시 기록을 유지하여야 하며, 물리적 보안 담당자는 주기적으로 권한 및 운영의 적정성을 검토하여야 한다.

제13조 (전산장비 보안)
전산장비 설치 시에는 불필요한 접근 및 위험을 최소화하도록 배치하고 필요한 통제수단을 도입하여야 한다.

제14조 (전산 시설 보호)
환경적, 자연적 위협으로부터 건물 및 시설을 보호하기 위해 방재, 방화, 항온·항습, 케이블 보호, 랙 실장도 관리, 비상전원 설비 등을 갖추어 최적의 상태를 유지하여야 하고 한다.

제15조 (사무실 보호 대책)

① 사무실 보안관리 현황을 주기적으로 점검하며, 비밀 정보는 반드시 잠금 장치가 되어 있는 장소에 보관한다.
② 프린터, 팩스, 복사기의 사용 시 산출되는 문서는 즉시 회수함으로써 출력물을 타인이 가져가게 하거나, 프린터 주위에 출력물이 방치되지 않도록 하여야 한다.

보안사고 대응

제16조 (보안사고의 예방 및 대응)

① 회사는 보안사고를 사전에 예방하고 대응할 수 있도록 통제 대책을 수립하고 적용하여야 한다.
② 보안사고를 인지한 임직원은 정보보호 담당자에게 즉시 신고하여야 하며 보안사고 발생 시 사고 대응을 위한 조직을 구성하여 대응책을 적용하여야 한다.
③ 보안사고의 예방 및 대응에 관한 세부 사항은 '보안사고 대응 지침'을 따른다.

보안 점검 및 감사

제17조 (보안 점검 및 감사 준수 관리)

① 정보보호 담당자는 정보보호 규정 및 유관 법령에서 정하는 항목의 준수 여부를 확

인하기 위하여 아래와 같은 영역에 대해 연1회 이상 보안 점검 및 감사를 수행한다.

1. 정보보호 규정의 준수 여부
2. 정보보호 관련 법률 등의 준수 여부
3. 정보자산에 대한 침해 위험 대응 여부
4. 기타 필요하다고 판단되는 영역

② 보안 점검 및 감사 결과에 따른 지적 사항은 즉시 해결될 수 있도록 하며, 차후 보안 점검 및 감사 시 기존 이행 점검 결과에 따른 조치 상황을 우선 검토한다

제18조 (점검 및 감사 결과의 처리)

① 보안 점검 및 감사 결과에 따른 지적 사항은 각 부서 및 부서장 책임 하에 즉시 해결될 수 있도록 한다.

② 차후 보안 점검 및 감사 시 기존 이행 점검 결과에 따른 조치 상황을 우선으로 검토한다.

③ 보안 점검 및 감사결과 준수 성과가 뛰어난 부서나 개인에게는 포상하고, 위반사항이 많은 부서나 개인에게는 처벌할 수 있다.

부 칙

제1조 (시행일)

본 규정은 공포일을 시행일로 한다.