

개인기기 사용 지원 (Bring Your Own Device, BYOD) 정책

1- 개요

[단체 이름] (이하 “단체”)는 직원/사용자에게 (이하 “사용자”) 스마트 기기를 (이하 “기기”) 사용할 권리를 부여하며, 이 기기는 핸드폰, 태블릿, 패블릿, 스마트워치, 스마트 카메라 등을 포함하나 이에 한정되진 않는다. [단체 이름]은 사용자가 아래 명시된 정책 및 절차에 따르지 않을 시, 또는 정책이 변할 시 이 권리를 철회할 수 있다.

[단체 이름]의 직원은 회사 네트워크에 개인기기를 연결하기 위해서는 이 정책에 명시된 다음 이용약관에 반드시 동의해야 한다.

2- 목적

이 정책은 [단체 이름]의 자료 및 기술 인프라에 대한 보안과 무결성을 보호하기 위해 존재한다. 기기 및 플랫폼의 다양성으로 인해 이 정책에 대한 제한적인 예외가 발생할 수도 있다.

3- 범위

이 정책은 [단체 이름]의 네트워크에 연결된 모든 기기의 적절한 사용을 다루며, 모든 직원, 공급 업체, 인턴 및 대리인이 [단체 이름]을 대신하여 업무를 할 때 적용된다.

4- 정책

- a) [단체 이름]은 허용 가능한 업무 사용을 [단체 이름]의 사업을 위해 직간접적으로 지원하는 활동이라고 정의한다.
- b) [단체 이름]은 허용 가능한 회사 업무시간의 개인적 사용을 합리적이고 제한된 개인적인 의사소통 또는 독서 및 게임 등 오락 활동이라고 정의한다.
- c) 직원들은 업무 시간 내, [단체 이름]의 네트워크에 연결된 동안 특정 웹사이트에 접근하지 못하도록 차단되어 있다. 이러한 웹사이트들은 음란물, 해적판 소프트웨어, 도박 및/또는 국제적 또는 지역 법에 따른 불법 콘텐츠를 포함하나, 이에 한정되진 않는다.
- d) 사용자들은 4.c 조항에서 언급된 웹사이트 및 장치의 보안을 위해 설치된 다른 컨트롤을 우회하여 접근하기 위해 소프트웨어/하드웨어 도구들을 사용해선 안 된다.
- e) 현장에서 기기들의 카메라 및/또는 영상 기능은 비활성화되지 않는다.
- f) 기기를 사용해서 안되는 경우는 다음과 같다:
 - a. 불법자료의 저장 또는 전송
 - b. [단체 이름]의 독점 정보의 저장 또는 전송
 - c. 타 회사의 독점 정보의 저장 또는 전송
 - d. 괴롭힘
 - e. 외부 사업 활동
 - f. 불법 활동

- g) 직원들은 다음과 같은 경우에만 자신의 기기를 활용하여 회사가 보유한 자료(이메일, 캘린더, 연락처, 문서 등)에 접근할 수 있다.
- a. 악성코드의 부재
 - b. 안티바이러스 소프트웨어 설치 (활성화되어있고, 작동 가능하며, 업데이트되어있음)
 - c. 전체 디스크 암호화 사용
 - d. 화면 잠금 사용
 - e. 원격 삭제 기술 (IT 지원 담당자에게 문의)
- h) [단체 이름은] 자동차 주행 중 문자 메시지 또는 이메일 전송에 대하여 무관용 (zero-tolerance) 정책을 시행하고 있으며 운전 중에는 핸드프리 대화만 허용된다.
- i) 이 정책을 준수하지 않을 시 사용자의 개인적인 책임이 발생할 수도 있다. 만약 사용자가 정책을 준수하지 않는다는 것이 판명될 경우, 사용자는 내부 규정이나 관련 법규에 따른 법적 절차에 따라 징계 처분을 받을 수 있다.

나는 [단체 이름]의 “개인기기 사용 지원”을 읽었으며 [단체 이름]에 계속하여 고용되기 위한 조건 중 하나로 이에 따를 것을 동의한다. 나는 위 정책을 위반할 경우 해고될 수도 있단 걸 이해한다.

사용자 서명

날짜