원격 액세스 정책

1- 개요

팀의 생산성을 유지하기 위해선 회사 네트워크에 원격으로 접근할 수 있는 게 매우 중요하나, 많은 경우 이러한 원격 액세스는 이미 보안이 훼손되었거나 본 회사의 네트워크보다는 현저히 낮은 보안상태에 있다. 이러한 원격 네트워크는 [단체 이름] 정책의 통제범위를 넘어서는 것이지만, 우리는 이러한 외부 위험을 우리 능력 선에서 최대한 줄여야 한다.

2- 목적

이 정책의 목적은 모든 호스트에서 [단체 이름]의 네트워크에 연결할 때 필요한 규칙과 필요조건들을 정의함에 있다. 이러한 규칙과 필요조건은 [단체 이름]의 자원을 무단으로 사용해서 발생할 수 있는 손상을 최소화하기 위해 만들어졌다. 손상은 민감한 또는 회사의 기밀 자료의 손실, 지적 재산, 공공 이미지 손상, [단체 이름]의 내부 시스템에 치명적인 손상 및 이러한 손실의 결과로 발생한 벌금이나 다른 금융 부채를 포함한다.

3- 범위

이 정책은 [단체 이름]의 네트워크에 접근하기 위하여 [단체 이름] 또는 개인이 소유한 컴퓨터나 워크 스테이션을 사용하는 [단체 이름]의 직원, 계약자, 인턴, 공급업체 및 에이전트에게 적용된다. 이 정책은 이메일을 읽거나 보내고 인트라넷 웹 자료를 보는 것을 포함한, [단체 이름]을 위한 작업 시 사용되는 원격 액세스 연결에 적용된다. 이 정책은 [단체 이름]의 네트워크에 연결하기 위해 사용하는 그 어떤 또는 모든 원격 액세스 기술의 구현을 다룬다.

4- 정책

[단체 이름]의 네트워크를 통해 여가 용도로 인터넷에 일반적인 접근을 할 수 있는 건 [단체 이름]의 직원, 계약자, 공급 업체, 인턴 및 에이전트 (이하 “허가받은 사용자”)로 제한한다. “허가받은 사용자”가 개인 컴퓨터에서 [단체 이름]의 네트워크에 접근할 시, “허가받은 사용자”가 아닌 사용자들이 [단체 이름]의 컴퓨터 자원 및 데이터에 대해 접근하는 걸 막을 책임이 있다. [단체 이름]의 네트워크를 통한 불법적 행위는 모든 사용자(“허가받은 사용자” 또는 그 외 사용자)에게 금지되어있다. “허가받은 사용자”는 본인의 액세스 오남용에 대한 책임과 결과를 지닌다.

“허가받은 사용자”는 외부 사업 이익(outside business interests)을 위해 [단체 이름]의 네트워크를 사용하지 않는다.

원격 액세스 로그인, 무료 바이러스 백신 소프트웨어, 문제 해결 지원 등 [단체 이름]의 원격 지원 연결 옵션과 관련된 추가 정보에 대해서는 IT 지원팀에 문의한다.

a. 필요 조건

i. 안전한 원격 액세스는 암호화(예: VPN)와 강력한 패스프레이즈로 엄격히 통제되어야 한다.
ii. “허가받은 사용자”는 설령 가족구성원 이라 할지라도 로그인과 암호를 보호해야 한다.
iii. [단체 이름] 소유의 컴퓨터를 사용하여 [단체 이름]의 네트워크에 원격으로 접근할 시, “허가받은 사용자”는 원격 호스트가 동시에 다른 네트워크에 연결되어 있지 않도록 해야한다. 단, 본인 또는 “허가받은 사용자” 또는 “제3자”의 완전한 통제하에 있는 개인 네트워크는 예외이다.
iv. [단체 이름]의 사업을 수행하기 위해 외부 자원을 사용하기 위해선 적절한 사업부 관리자에게 사전에 승인을 받아야 한다.
v. 원격 액세스 기술을 사용하여 [단체 이름]의 내부 네트워크에 접속한 모든 호스트들은 최신 바이러스 백신 소프트웨어와 방화벽 소프트웨어를 사용해야 한다. 제3자는 제3자 계약에 명시된 요구 사항을 준수해야 한다.
vi. [단체 이름]의 네트워크에 접속하기 위해 사용하는 개인 장비는 반드시 [단체 이름]의 네트워크에 접속하기 위한 “원격 액세스 정책”의 정보 보안 정책 조건들을 충족해야 한다.

나는 [단체 이름]의 “원격 액세스 정책”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