

무선 통신 표준

1- 개요

“목적” 참고.

2- 목적

이 표준은 [단체 이름]의 네트워크에 연결하기 위해 무선 인프라 장치가 충족시켜야 하는 기술적 조건을 지정한다. 이 표준에 명시된 조건을 충족하거나 InfoSec 팀에 의해 예외로 지정된 무선 인프라 장치들만이 [단체 이름] 네트워크 연결에 대한 승인을 받을 수 있다..

허브, 라우터, 스위치, 방화벽, 원격 액세스 장치, 모뎀, 무선 액세스 지점을 포함하되 이에 국한되지 않는 네트워크 장치들은 정보 보안 컨설턴트가 승인한 서포트 조직에 의해 설치, 지원 및 유지 관리가 되어야만 한다.

3- 범위

이 정책은 [단체 이름] 및 자회사에서 일하거나 함께 일하는 직원, 계약자, 인턴, 공급업체 및 에이전트들에게 적용되며, [단체 이름]을 대표하여 무선 인프라 장치를 유지 관리하는 모든 직원을 포하고, 이들은 이러한 표준을 준수해야 한다. 이 표준은 네트워크와 연결되는 모든 무선 장치와 네트워크에 무선연결을 제공하는 모든 무선 인프라 장치에 적용된다.

4- 표준

4.1 일반적인 필요 조건

[단체 이름]의 네트워크에 연결되거나 [단체 이름]의 기밀 (Confidential), [단체 이름]의 고위 기밀 (Highly Confidential), 또는 [단체 이름]의 제한 (Restricted) 정보에 대한 액세스를 제공하는 모든 무선 인프라 장치들은 반드시 다음과 같아야 한다:

- EAP-FAST (Extensible Authentication Protocol-Fast Authentication via Secure Tunneling), PEAP (Protected Extensible Authentication Protocol), 또는 EAP-TLS (Extensible Authentication Protocol-Translation Layer Security)을 인증 프로토콜로 사용한다.
- 최소한 256 비트의 키 길이를 가진 Temporal Key Integrity Protocol (TKIP) 또는 Advanced Encryption System (AES) 프로토콜 둘을 사용한다.
- 모든 블루투스 장치들은 암호화가 활성화된 SSP (Secure Simple Pairing)를 사용해야 한다.

4.2 게스트 사용자 및 격리된 무선장치 필요조건

- 게스트 사용자들의 SSID (WiFi Service Set Identifier)는 반드시 [단체 이름]의 생산 장치 SSID와 달라야 한다.

- 게스트 사용자들의 네트워크는 반드시 [단체 이름]의 네트워크에서 분리되어 있어야 한다.

4.3 가정용 무선장치 요구사항

[단체 이름]의 네트워크에 직접 접근을 허용하는 모든 가정용 무선 인프라 장치들은 (예를 들어 ECT (Enterprise Teleworker) 또는 하드웨어 VPN 등을 위한 장치들) 다음 사항을 준수해야 한다:

- WPA-PSK (WiFi Protected Access Pre-shared Key), EAP-FAST, PEAP, 또는 EAP-TLS 을 활성화한다
- WPA-PSK을 활성화 할 때, 무선 클라이언트와 무선 액세스 포인트에서 공유하는 복잡한 비밀 키 (최소 20자)를 구성한다
- SSID의 브로드캐스트 비활성화
- 기본 SSID 이름 변경
- 기본설정된 로그인 및 암호 변경

나는 [단체 이름]의 “무선 통신 표준”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