|  |  |
| --- | --- |
| **Document Name** | **Wireless Network Policy** |
| **Version** | **0.2** |
| **Created By** | **Dushyant S. Gupta** |
| **Revised By** | **Anjaly T A** |
| **Reviewed By** |  |
| **Released on** |  |

Contents

[Purpose 3](#_Toc61445753)

[Scope 3](#_Toc61445754)

[Policy 3](#_Toc61445755)

[Wireless Deployments 3](#_Toc61445756)

[Restrictions: 4](#_Toc61445757)

[**Enforcement** 4](#_Toc61445758)

# **Purpose**

The purpose of this policy is to secure and protect the information assets owned by Xtracap. Xtracap provides computer devices, networks, and other electronic information systems to meet its mission, goals, and objectives. Xtracap grants access to these resources according to an individual’s role and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This policy specifies the conditions that wireless infrastructure devices must satisfy in order to connect to the Xtracap network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by CISO are approved for connection to the Xtracap network.

# **Scope**

This policy addresses the requirements of Wireless deployments, Wireless usage, and Wireless airspace usage. All employees, contractors, consultants, temporary workers, and others who use the Xtracap network, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Xtracap, must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to the Xtracap network or reside at an Xtracap owned, leased or rented site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

# **Policy**

## Wireless Deployments

**Standards supported:**

IEEE 802.11ac and 802.11n are the preferred wireless networking standards. 802.11g, 802.11b, and 802.11a will be available, where necessary.

IEEE 802.1X is the authentication standard. Additional security procedures may be applied as needed.

WPA2 with AES encryption will be the only secure standard used.

**Service Set Identifier (SSID):** There shall be three SSIDs broadcast by the wireless deployment. Only devices authenticated account credentials may access this SSID.

**Wireless Service Considerations:**

Wireless networking has bandwidth limitations compared to the wired network. The wireless network should be viewed as augmenting the wired network, to provide more flexible network use. Applications that require large amounts of bandwidth, or are sensitive to changes in signal quality and strength may not be appropriate for wireless access.

Wireless technology is and will for the foreseeable future be a shared bandwidth technology. Some protocols and services will not effectively work in, or may be inappropriate for, a wireless environment.

DHCP is the standard addressing method for the IC wireless networks, and is expected to meet the majority of customer requirements.

Wireless is a dynamic service. Due to the dynamic nature of wireless, IP space serving the campus will change over time due to capacity re-engineering.

# **Restrictions**

Xtracap policy requires that all deployments of wireless infrastructure be installed and maintained by DIIS. Installing departmental or do-it-yourself wireless access points is prohibited to avoid possible interference with the IC wireless network, unnecessary impact to the wired network and to minimize undue security risks to the company. Additionally, in areas where centrally-managed wireless networking is available any pre-existing locally managed access points must be removed.

* Use of the wireless network is subject to the established policies for use of network services.
* Only devices authenticated via Xtracap account credentials may access network resources on its network that are not Internet facing.

# **Enforcement**

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy