Wireless Security Policy

1. Overview

With the mass explosion of Wi-Fi capable devices, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat factors.

2. Purpose

The purpose of this policy is to secure and protect the information assets owned by Hillcrest School District. The district provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Hillcrest School District grants access to these resources as a privilege 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 to connect to Hillcrest School District network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Technology Department are approved for connectivity to the network.

3. Scope

All employees, students, contractors, consultants, temporary and other workers at Hillcrest School District including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Hillcrest School District must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a Hillcrest School District network or reside on a Hillcrest School District site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

4. Policy

4.1 General Requirements

All wireless infrastructure devices that reside at a Hillcrest School District site and connect to a Hillcrest School District network, or provide access to information classified as Hillcrest School District Confidential, or above must:

- Be approved by the IT Director before connecting to schools Wi-Fi network.
- Register your devices MAC Address with the IT Director.
- Use Hillcrest School District approved encrypted authentication protocols and infrastructure, WPA2 Enterprise/Personal or MAC address authentication
- Not interfere with wireless access devices.

5. Policy Compliance

5.1 Compliance Measurement

The IT Director will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, and internal and external audits.

5.2 Exceptions

The IT Director must approve any exception to the policy in advance.

5.3 Non-Compliance

Any user found to have violated this policy might be subject to disciplinary action.

6 Related Standards, Policies and Processes

- Personnel Internet & Computer Use Policy
- Student Internet & Computer Use Policy

7 Revision History

Date of Change	Responsible	Summary of Change
January 2015	IT Director	Updated policy.
July 2016	**IT Director**	**Updated policy**