Wireless Communication Policy

POLICY: The purpose of this policy is to secure and protect the information assets owned by Black Hawk County. Black Hawk County provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Black Hawk County grants access to these resources voluntarily and users 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 the Black Hawk County 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 a Black Hawk County network.

SCOPE: All employees, contractors, consultants, temporary and other workers at Black Hawk County including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Black Hawk County must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a Black Hawk County network or reside on a Black Hawk County 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.

DEFINITIONS: Mac Address is defined as a physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

REQUIREMENTS: All wireless infrastructure devices that reside at a Black Hawk County site and connect to a Black Hawk County network, or provide access to information classified as Black Hawk County Confidential, or above must:

- Abide by the standards specified in Information Technology's *Wireless Communication Standard*.
- Be installed, supported, and maintained by an approved support team.
- Use Black Hawk County approved authentication protocols and infrastructure.
- Use Black Hawk County approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

ISOLATED WIRELESS DEVICE REQUIREMENTS: Isolated wireless devices that do not provide general network connectivity to the Black Hawk County network must:

- Be isolated from the county network (that is it must not provide any county connectivity).
- Not interfere with wireless access deployments maintained by other support organizations.

HOME WIRELESS DEVICE REQUIREMENTS: Employees should reference the Virtual Private Network (VPN) Policy for guidelines on appropriate home wireless device requirements.

COMPLIANCE MEASUREMENTS: The Information Technology Department will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback. Any exception to the policy must be approved by the Information Technology Department in advance. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.