

# Wireless Communication Practice

Author:

Reviewers:

Approvers:

## Version History

<b>Date</b>	<b>Version Number</b>	<b>Name</b>	<b>Reason</b>
5/14/2003	1.00		Original version
4/17/2006	1.01	Bob Boyd	Revised to update terminology related to County Policies.

## **1. Purpose**

The purpose of this practice is to ensure the protection of Johnson County's information and information systems against damage, misuse or unauthorized disclosure of any kind.

## **2. Scope**

This practice applies to all employees, contractors, consultants, temporary employees, vendors, other government agencies and other users of Johnson County's information systems, including computer servers, networks, personal computers, laptops, PDA devices, mainframe systems and other electronic devices that may store or transfer Johnson County information.

## **3. Statement**

Regardless of the security measures employed, wireless data communications are inherently less secure than wired communications. Wireless network signals can often be intercepted from public areas within a building or even outside at distances as much as a mile or more. Encryption and authentication schemes can be circumvented unless properly implemented.

Any County department seeking to implement a wireless network solution should strongly consider the business case for the proposed solution. In many instances, the convenience may not be worth the risk. Wireless networks are also very easy to disrupt or "jam", making wireless solutions poor choices for mission critical applications.

Therefore, the implementation of wireless network solutions to allow access to the Johnson County trusted network is strictly prohibited except under the conditions stipulated in this practice.

## **4. Definitions**

- A. Authentication:** The process of verifying that an individual user is who he presents himself to be before granting him access to network resources.
- B. Network:** An interconnected system of computers that facilitate the sharing of information and devices among local and remote users.
- C. RADIUS (Remote Authentication Dial-In User Service):** A system used to authenticate remote users and allow or deny them access to a network or computer system.
- D. TACACS+ (Terminal Access Controller Access Control System):** A system used to authenticate remote users and allow or deny them access to a network or computer system.
- E. Trusted Network:** Any group of computers that are directly connected to the County's network with no firewall or other security device in place to regulate or monitor the data that passes back and forth to the County network.
- F. User:** Johnson County employees, temporary workers, consultants, vendors, volunteers and other individuals who use County computer systems.

## **5. Roles and Responsibilities**

### **A. Information Technology Services**

The ITS Department is responsible for providing guidance and assistance in selecting the necessary hardware and configuration parameters for establishing secure wireless networks. ITS is further responsible for providing and maintaining security practices and usage guidelines related to wireless networks. The ITS Department also provides RADIUS authentication services that may be utilized to authenticate wireless users.

### **B. Appropriate Management**

Appropriate Management is responsible for establishing office, agency or departmental procedures and practices that are consistent with this Policy. Appropriate Management is further responsible for advising employees and all other users about this Policy and the appropriate use of County systems.

## **6. Standards**

### **A. ENCRYPTION**

All wireless communications must be encrypted with wireless encryption protocol (WEP) or equivalent encryption scheme using no less than 128-bit keys. Encryption (WEP) keys must be changed in a regular and automated fashion at intervals of less than 60 minutes.

### **B. ANTENNAS**

Wireless antennas and equipment must be configured and physically located in a configuration that will minimize network signal outside the intended area. For wireless LAN (WLAN) implementations, technical support staff in the specific department or from the ITS Department should verify signal strength outside the physical office space where the wireless network resides.

### **C. AUTHENTICATION**

Strong user authentication, such as RADIUS or TACACS+ must be employed with all wireless network solutions. Johnson County ITS maintains RADIUS systems that may be utilized in many cases.

### **D. SSID BROADCAST**

When possible, wireless networks should be configured not to broadcast or “beacon” network identifying information, such as the Service Set Identifier (SSID). If the SSID must be broadcast, a non-identifiable or cryptic SSID should be chosen. For example, use “ZZ123” rather than “JOCO ITS” or “CISCO1200”.

### **E. ROGUE WIRELESS NETWORKS**

The Johnson County ITS Director should be made aware of any wireless network on the Johnson County trusted network. In addition, County departments should ensure that employees do not establish unauthorized, “rogue,” wireless network segments within the County network. The ITS Department will conduct periodic audits to detect unsecured and unauthorized wireless networks.

### **F. PEER-TO-PEER WIRELESS**

Many wireless network cards include a feature that allows computer workstations to

communicate with each other directly via their wireless interface. This is known as “peer-to-peer” connectivity, and it presents another serious security risk. Care must be taken to always disable “peer-to-peer” wireless communications.

## **7. History**

This is a new practice.