names and passwords are removed from the device. Administration of the device will be prohibited from the wireless network.

1.2.3 Authentication and Encryption

Authentication and encryption is required on all WLANs (see options listed on the registration form for details).

1.2.3.1 Access to Systems and Data

- Agencies and other entities connected to the state's network must employ adequate security measures to protect other systems and data connected to the state's network.
- Once authenticated to an access point, users will either be routed outside the state's firewall(s), or authenticated to the network. Just as with a wired network, state network authentication--whether enterprise-wide or agency-specific-- must satisfy prescribed login/password combinations prior to using enterprise or agency-specific resources that are not normally accessible by nodes outside the state's firewall(s).
    - For users requiring only an Internet connection (i.e. vendors, customers, and citizens) authentication to an access point may be made through the use of a Guest account. This account must still provide authentication but the account may be reused or shared on an as needed basis. Passwords on Guest accounts should be changed frequently.
- Access control mechanisms such as firewalls must be deployed to separate the wireless network from the internal wired network.
- As the technology permits, wireless networks will employ a combination of layered authentication methods to protect sensitive, proprietary, and patient information.

1.2.4 Risk Management

Agencies using wireless systems must develop general risk mitigation strategies for access points, users, and client devices such as virus protection, password standards, and other preventative measures.

1.3 Disruption and Interference

For state agencies, the DOC will resolve any conflicts between wireless devices in coordination with the affected agencies. Priority is granted to fully supported and registered installations, except in the case of medical, safety, or emergency devices, as appropriate.

1.4 Compliance with Other Network Standards

Agency WLANs must satisfy all existing and future standards pertaining to use and security of the state's network as required by law or established by the Nebraska Information Technology Commission or ITS.

1.5 General Recommendations for Agencies Implementing WLANs

1.5.1 Agencies must not undertake wireless deployment until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of operations. Agencies should perform a periodic risk assessment and