



County of Ottawa

WIRELESS ACCESS POLICY

I. POLICY

Access to County of Ottawa networks via unsecured wireless communications mechanisms is prohibited. Only wireless systems installed and supported by the County Information Technology (IT) Department are authorized for wireless access within the County. Wireless access is not intended to be the primary mode of communication, except in cases where it is the most cost effective method to conduct business. Wireless devices and networks without connectivity to the County network do not fall under the purview of this policy.

II. STATUTORY REFERENCES

None.

III. COUNTY LEGISLATIVE OR HISTORICAL REFERENCES

Board of Commissioners Resolution Number and Policy Adoption Date: _____

Board of Commissioners Review Date and Resolution Number: _____

Name and Date of Last Committee Review: _____



County of Ottawa

WIRELESS ACCESS POLICY

PROCEDURE

1. All wireless access points/base stations connected to the County network must be registered and approved by the IT Security Officer. All wireless Network Interface Cards (NIC/PC Cards) used in corporate or desktop computers must be registered with the IT Security Officer.
2. All wireless LAN access must use County approved vendor products and security configurations. The use of personal wireless access devices is prohibited.
3. All computers with wireless LAN devices must utilize County approved authentication and encryption protocols.
4. Non-County employees requiring access to County wireless connections will submit a written request including name, contact information, agency and justification to the responsible/supported department head or elected official. Endorsed requests will be forwarded to the IT Department for final review and approval. Requests not meeting these requirements and technology that is incompatible will be rejected. Requesters approved for access will deliver their equipment to the IT Department for configuration and testing.
5. The loss of any equipment configured to access County Wireless connections or change in ownership will be reported immediately to the IT Department Security Officer and service for that device will be terminated.
6. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

REVIEW PERIOD

The Information Technology Director will review these policies and procedures and report to the Planning and Policy Committee at least once every two years.