



County of Ottawa

REMOTE ACCESS AND APPLICATION SERVICE PROVIDER POLICY

I. POLICY

It is the responsibility of County of Ottawa employees, contractors, vendors and agents with remote access privileges to the County network to ensure that their remote access connection uses the secure methods of connection made available by the Information Technology (IT) Department. Any method of connectivity that circumvents security by an unsecured means or allows unauthorized persons access to the County network is prohibited. Remote access implementations that are covered by this policy include but are not limited to dial-in, frame relay, ISDN, DSL, Wireless, VPN, SSH, cable and Extranet.

In addition, any Application Service Provider (ASP) engaged by the County must comply with all security requirements and policies regardless of where the application is hosted.

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 COUNTY LEGISLATIVE OR HISTORICAL REFERENCES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

REMOTE ACCESS AND APPLICATION SERVICE PROVIDER POLICY

PROCEDURE

1. Secure remote access is strictly for employees and authorized vendors, contractors and agents of the County of Ottawa. Anyone authorized for remote access should at no time allow any unauthorized individual to use their connection, nor share their password, or other information needed to gain access.
2. County employees and contractors with remote access privileges must ensure that their County owned or any personal computer which is remotely connected to the County's network is not connected to any other network at the same time with the exception of personal networks that are under the complete control of the user.
3. County employees must not use non-County e-mail accounts to conduct County business, thereby ensuring that official business is never confused with personal business.
4. Reconfiguration of a home computer user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
5. All hosts (including personal computers) that are connected to the County internal networks via remote access technologies must use the most up-to-date antivirus software.
6. This policy applies to all devices that access the County network which could include PC's, Laptops, Servers, PDA's, WAP phones, etc.
7. Application Service Providers must provide documented proof of compliance with acceptable information security requirements. Any information hosted by an ASP is the property of the County and disclosure of information to any non-County entity will only be with written authorization from the IT Director. No restrictions will be placed on the County's access to that information.
8. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
9. Any ASP found to have violated this or any other County policy may be subject to legal action.

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.