Category: 100
Number: 138

Subject: **REMOTE ACCESS POLICY**

1. PURPOSE: It is the purpose of this policy to define standards, procedures, and restrictions for connecting to Saginaw County's network(s) from external hosts via remote access technology.

2. AUTHORITY: The Saginaw County Board of Commissioners.

3. APPLICATION: This policy applies to, but is not limited to, all Saginaw County employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize company- or personally-owned computers to remotely access the organization's data and networks. Employment and/or affiliation with Saginaw County do not automatically guarantee the granting of remote access privileges.

    3.1 Any and all work performed for Saginaw County on said computers by any authorized remote users through a remote access connection of any kind, is covered by this policy. Work can include (but is not limited to) e-mail correspondence, Web browsing, utilizing intranet resources, and any other company application used over the Internet. Remote access is defined as any connection to Saginaw County's network and/or other applications from off-site locations, such as the employee's home, a hotel room, airports, cafés, satellite office, wireless devices, etc., pursuant to Policy #138.

4. RESPONSIBILITY: The Saginaw County Information Systems and Services Department (SCISS) of the Saginaw County Controller's Office shall be responsible for the implementation and enforcement of this policy.

5. DEFINITIONS: NONE

6. POLICY:

    6.1 Supported Technology

        6.1.1 All remote access will be centrally managed by Saginaw County's Information Systems and Services (SCISS) department and will utilize encryption and strong authentication measures. Remote access connections covered by this policy include (but are not limited to) Internet dial-up modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, proprietary remote access/control software, etc.

6.1.2 Saginaw County requires all client hardware and software to conform to its security standards. While a variety of computer hardware and software platforms are available to use for connections, not all combinations will meet Saginaw County's standards; computer equipment that is not able to meet the standards set by SCISS will not be allowed to participate in remote access sessions.

6.1.3 Saginaw County ISS staff may work with users, providing minimal support and hardware/software recommendations. However, it is the responsibility of the remote access user to allocate hardware and software support, as needed, for problems beyond the immediate scope of the remote access connection; SCISS reserves the right to define said scope. If deemed necessary, users with hardware/software problems may have their remote access service suspended, pending the completion of necessary computer repairs, if ISS has deemed the equipment a security threat. It is the user's responsibility to advise SCISS when their equipment is in for service, to insure that remote access for that device is removed, pending return of the equipment to the user.

6.2 Eligible Users

6.2.1 All users requiring the use of remote access for business purposes must go through an application process that clearly outlines why the access is required and what level of service the user needs should his/her application be accepted. Application forms must be approved and signed by the employee's unit manager, supervisor, or department head before submission to the SCISS department.

6.2.2 Users may use privately owned connections (under 'Supported Technology') for business purposes. If this is the case, the SCISS department must approve the connection as being secure and protected. However, Saginaw County's ISS department cannot and will not technically support a third-party ISP connection or hotspot wireless ISP connection; this includes computers and other non-county equipment. All expense forms for reimbursement of cost (if any) incurred due to remote access for business purposes (i.e. Internet connectivity charges) must be submitted to the appropriate unit or department head. Financial reimbursement for remote access is not the responsibility of the SCISS department.

6.3 Appropriate Use

6.3.1 It is the responsibility of any user with remote access privileges to ensure that their remote access connection remains as secure as his or her network access within the office. It is imperative that any remote access connection used to conduct Saginaw County business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

6.3.2 The use of wireless network equipment by approved remote access users brings with it certain security risks, and therefore must be pre-approved (certified) by Saginaw County ISS, prior to receiving remote access; the addition of associated hardware by an approved user, without prior notification and approval by SCISS, is prohibited, and may result in the suspension of remote access privileges.

6.3.3 Remote access users will use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Saginaw County's password policy. Authorized remote users agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home. Disclosure of this information to others is a direct violation of this policy and will result in immediate loss of remote access privileges.

6.3.4 All remote computer equipment and devices used for business interests, whether personal- or company-owned, must display reasonable physical security measures. Computers will have installed whatever antivirus software deemed necessary by Saginaw County's SCISS department. Users with High-Speed Internet connections such as, but not limited to, DSL/CABLE/ISDN, will need to be utilizing a hardware and/or software Firewall, subject to evaluation by Saginaw County ISS.

6.3.5 Remote users using public hotspots for wireless Internet access must employ for their devices a company-approved personal firewall, VPN, and any other security measure deemed necessary by the SCISS department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Saginaw County's additional security measures. VPN connections will be configured with no less than 128-bit encryption, configured as deemed necessary by SCISS. Users must maintain password security, changing passwords with a frequency and manner that is consistent with the currently established password security policy, as managed and maintained by SCISS.

6.3.6 Any remote connection (i.e. hotspot, ISDN, frame relay, etc.) that is configured to access Saginaw County resources must adhere to the authentication requirements of Saginaw County's ISS department; in addition, all hardware security configurations (personal or company-owned) must be approved by Saginaw County's ISS department.

6.3.7 No authorized remote user will make any modifications of any kind to the remote access connection without the express approval of Saginaw County's ISS department. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations, etc.

6.3.8 In order to avoid confusing official company business with personal communications, users with remote access privileges must never use non-company e-mail accounts to conduct Saginaw County business.

6.3.9 No authorized remote user is to use Internet access through company networks via remote connection for the purpose of illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other existing Saginaw County policies.

6.3.10 All remote access connections must include a "time-out" system. In accordance with Saginaw County's security policies, remote access sessions will time out after 20 minutes of inactivity, and will terminate after two (2) hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter Saginaw County's networks. Should a remote user's account be inactive for a period of 30 days, access account privileges will be suspended until the SCISS department is notified.

6.3.11 If a personally - or company-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized remote user will be responsible for notifying their manager and Saginaw County's ISS department immediately.

6.3.12 The authorized remote access user also agrees to immediately report to their manager and Saginaw County's ISS department any incident or suspected incidents of unauthorized access and/or disclosure of Saginaw County company resources, databases, networks, etc.

6.3.13 The authorized remote access user also agrees to and accepts that his or her access and/or connection to Saginaw County's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-

house computers, this is done in order to identify accounts/computers that may have been compromised by unauthorized parties.

6.3.14 Saginaw County will not reimburse remote access users for business-related remote access connections made on a pre-approved privately owned ISP service.

6.4 Non-Compliance

6.4.1 Failure to comply with the Remote Access Policy and Agreement may result in the temporary or permanent loss of remote access privileges, legal or disciplinary action, and possibly termination of employment or Saginaw County business relationships.

7. ADMINISTRATIVE PROCEDURES: The Information Systems and Services Department of the Saginaw County Controller's Office shall be responsible for the implementation and enforcement of this policy; and to ensure the highest security levels are maintained to protect Saginaw County's databases and network infrastructure.

8. CONTROLLER/CAO LEGAL COUNSEL REVIEW: The Controller/CAO has determined that this Policy, as submitted to the Board of Commissioners, contains the necessary substance in order to carry out the purpose of the policy. County Civil Counsel has determined that this Policy, as submitted, contains content that appears to be legal activities of the Saginaw County Board of Commissioners.

Approved as to Substance:
Saginaw County Controller/CAO

Approved as to Legal Content:
Saginaw County Civil Counsel

ADOPTED: December 9, 2003