Remote Access Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for connecting to NNMC's internal network(s) from external hosts via remote access technology, and/or for utilizing the Internet for business purposes via third-party wireless Internet service providers (a.k.a. "hotspots"). NNMC's resources (i.e. corporate data, computer systems, networks, databases, etc.) must be protected from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all remote access and mobile privileges for NNMC employees to enterprise resources – and for wireless Internet access via hotspots – must employ only company-approved methods.

Scope

This policy applies to all NNMC 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 at NNMC does not automatically guarantee the granting of remote access privileges.

Any and all work performed for NNMC on said computers by any and all employees, 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 NNMC'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.

Supported Technology

All remote access will be centrally managed by NNMC's IT 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.

The following table outlines NNMC's minimum system requirements for a computer, workstation, or related device to comply with NNMC's systems. Those who do not meet these requirements must upgrade their machines, or face being denied remote access privileges.

	PC and PC-Compliant Computers	**Macintosh Computers**	**Handhelds, PDAs and Portables**

Operating System			
CPU			
RAM			
Disk Space			
Modem Type			

Eligible Users

All employees 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 employee 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 IT department.

Employees may use privately owned connections (under 'Supported Technology') for business purposes. If this is the case, the IT department must approve the connection as being secure and protected. However, the company's IT department cannot and will not technically support a third-party ISP connection or hotspot wireless ISP connection. 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 IT department.

Policy and Appropriate Use

It is the responsibility of any employee of NNMC 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 NNMC business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

1. General access to the Internet by residential remote users through NNMC's network is permitted. However, both the employee and his/her family members using the Internet for recreational purposes through company networks are not to violate any of NNMC's Internet acceptable use policies.

2. Employees will use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with NNMC's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

3. 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 NNMC's IT department.

4. 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 IT department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with NNMC's additional security measures.

    - Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, wardrivers, and eavesdroppers.
    - Users must apply new passwords every business/personal trip where company data is being utilized over a hotspot wireless service, or when a company device is used for personal Web browsing.

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

6. Employees, contractors, and temporary staff will make no modifications of any kind to the remote access connection without the express approval of NNMC's IT department. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations, etc.

7. Employees, contractors, and temporary staff with remote access privileges must ensure that their computers are not connected to any other network while connected to NNMC's network via remote access, with the obvious exception of Internet connectivity.

8. In order to avoid confusing official company business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-company e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct [company name] business.

9. No employee 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 employee policies.

10. All remote access connections must include a "time-out" system. In accordance with NNMC's security policies, remote access sessions will time out after 180 minutes of inactivity, and will terminate after unlimited hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter company networks.

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

12. The remote access user also agrees to immediately report to their manager and NNMC's IT department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

13. The remote access user also agrees to and accepts that his or her access and/or connection to NNMC'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 external parties.

14. NNMC will not reimburse employees for business-related remote access connections made on a pre-approved privately owned ISP service. All submissions for reimbursement must be accompanied by sufficient and appropriate documentation (i.e. original service bill). Employees requesting reimbursement will also be asked to certify in writing prior to reimbursement that they did not use the connection in any way that violates company policy.

Policy Non-Compliance

Failure to comply with the Remote Access Policy and Agreement may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

Employee Declaration

I, employee name_____, have read and understand the above Remote Access Policy and Agreement, and consent to adhere to the rules outlined therein.

_____	_____
Employee Signature	Date
_____	_____
Manager Signature	Date
_____	_____
IT Administrator Signature	Date