MWM Electronic Data Policies

MWM has implemented the following Electronic Data policies to ensure the security and privacy of electronic data. All MWM full and part-time employees, contractors, consultants, temps, assistants, volunteers, vendors, agents and other users including those affiliated with third parties who utilize MWM technology resources (for ease of reference only, all categories are collectively referred to herein as "Staff") are required to comply with these and other applicable MWM policies and procedures, as well as federal, state, local and/or international law.

Failure to abide by these conditions may result in forfeiture of the privilege to use technology resources, and disciplinary action (up to and including termination), and/or legal action.

Privacy
MWM retains the right to access, monitor, duplicate, record and/or log all staff use of MWM technology resources, with or without notice. This includes but is not limited to any and all e-mail (whether such account is maintained by MWM or a third party), internet access, keystrokes, file access, logins, and/or changes to access levels. **Staff shall have <u>NO expectation of privacy</u> in the use of MWM technology resources.**

Liability
MWM makes no warranties, whether express or implied, as a result of these policies. Moreover, MWM shall not be held responsible for any damage(s) to any Staff person resulting directly or indirectly from or otherwise related to the use of any MWM technology resource(s). ***All staff recognizes and agrees that the use of MWM technology resources is a privilege, and agrees to abide by all MWM Electronic Data policies.***

Staff Responsibility and Accountability
Effective information security requires Staff involvement as it relates to their jobs. Staff shall be accountable for all acts and/or any event resulting under their user identification code(s). It is Staff's responsibility to abide by the policies and procedures set forth herein, and to promptly notify MWM of any known or suspected violation of these policies and procedures. Access of personal or private Internet Service Providers while using MWM-provided information technology resources or using non-MWM provided information technology resources to conduct MWM business does not indemnify any Staff person from responsibility, accountability and/or compliance with any MWM policies. Staff responsibilities include but are not limited to:

- Data Control: Access and release only the data for which you have authorized privileges and a need to know (including misdirected e-mail)
- Know and follow all policies and laws (local, state, federal, and international) applicable to computer system use
- Promptly report known or suspected information security violations to the Information Security Officer or designee and cooperate fully with all investigations regarding the abuse or misuse of information technology resources
- Protect assigned user IDs, passwords, and other access keys from disclosure
- Secure and maintain confidential printed information, magnetic media or electronic storage mechanisms

in approved storage containers when not in use and dispose of these items in accordance with MWM policy
- Log off of systems (or initiate a password protected screensaver) before leaving a workstation unattended
- Use only MWM acquired and licensed software
- Follow all applicable procedures and policies

Enforcement
Violation of any MWM policy or procedure may result in disciplinary action, up to and including termination. Additionally, individuals who violate these policies may lose access privileges and, where applicable, face civil and/or criminal prosecution.

By signing below, you agree that you have received and reviewed the Electronic Data Policies contained herein, and agree that MWM has the right to enforce the policies and procedures, including but not limited to the following, as explained herein.

- Email & Internet Policy
- Acceptable Use Policy
- Anti-virus Policy
- Forwarded Email Policy
- Equipment Disposal Policy
- Password Policy
- Personal Communication Device Policy
- Remote Access Policy

Date:	
Name:	
Signature:	

I.

EMAIL & INTERNET POLICY

MWM's investment in information technology is intended to facilitate communication among and between MWM personnel and MWM's clients and other parties involved in the conduct of the MWM's business. This powerful technology creates both opportunities and risks. It is the responsibility of each Staff person to ensure that this technology is used prudently and properly, in a manner consistent with the following policies and procedures:

- MWM's electronic communications capacity is not unlimited. While they may be used for incidental personal communications, the Company's e-mail system and connection to the Internet are provided for business purposes and may not be used to engage in or communicate about improper or illegal activity such as computer "hacking," on-line gambling, illegal use, sale or distribution of controlled substances, interactive or other game playing, and personal shopping; connecting, posting, downloading, transmitting or storing offensive material and/or harassing or discriminatory material prohibited under MWM's Equal Opportunity, Anti-Sexual Harassment and Non-Discrimination policies; disabling or compromising the security of information contained on MWM's computers; and conducting, or soliciting for political, personal, religious or charitable causes or other commercial ventures outside the scope of the user's employment and the user's responsibilities to MWM.
- The e-mail and Internet systems must not be used to create, send, receive (download) or store any offensive materials or materials that are inconsistent with MWM's Equal Opportunity, Anti-Sexual Harassment and Non-Discrimination policies. Any materials that contain sexual implications, racial slurs, gender-specific comments, defamatory statements, or other comments that offensively addresses someone's age, race, color, religion, gender, age, nationality, national origin, sexual orientation, disability, marital status, veteran status, or any other characteristic protected by law, will not be tolerated.
- The e-mail system is MWM property, and all copies of messages created, sent, received or stored on MWM's system are and remain the property of MWM. They are not the private property of any Staff person irrespective of any such designation either by the sender or the recipient (including designation as "private", "personal" or "confidential").
- E-mails containing proprietary information of MWM should not be forwarded to third parties unless such parties have a business reason for receiving such information as a result of their business relationship with MWM. Copyright issues applicable to the electronic mail system are addressed below in this policy.
- By using MWM's electronic mail system, the Staff person recognizes and consents to the monitoring rights of MWM.. The contents of electronic mail may be disclosed within MWM and to third parties without further permission of the Staff person and at MWM's sole discretion.
- Notwithstanding MWM's right to retrieve and read any electronic mail message, such messages should be treated as confidential by individual Staff persons and accessed only by the intended recipient. No Staff person should attempt to gain access to a message of another person without the latter's permission. File passwords and codes, including encryption keys, must be disclosed to MWM and no such password, code or key may be used that is unknown to MWM. Any exception to this policy must receive prior written approval from the Office Manager.
- An individual may not subscribe directly to Internet list services. While list services can be valuable

business tools, it is possible for MWM to receive literally thousands of messages a day generated by list services, thus potentially overwhelming the system. Therefore, an individual user may not subscribe directly to a list service. MWM will subscribe to list services, and, by using the ability of MWM's e-mail system to distribute messages automatically, send any message received from a list service to all interested users. In order to avoid burdening MWM's system, any subscription to a list service must be limited to a business purpose. Any subscription to a list service must be coordinated with the Office Manager. Unauthorized subscriptions are subject to cancellation.

- Unless prior approval of the Office Manager has been obtained, a user may not establish an Internet or other external network connection using MWM property, or engage in any activity that could allow an unauthorized person to gain access to MWM's systems and information. These connections include the establishment of a separate Internet service electronic mail account or a host with a public modem dial-in, a website or World Wide Web home page, a File Transfer Protocol (FTP) or any other capability that makes information available for browsing, downloading or posting by a person who is not employed or engaged by MWM. An individual may not use Instant Messaging or Internet Relay Chat (IRC) products on MWM's systems. Any requested exception to this policy must receive prior written approval from the Office Manager.
- All other restrictions that apply to outgoing communications generally apply to communications via Internet chat rooms, bulletin boards and on-line discussion forums or groups as well.

All confidential, copyrighted and/or proprietary information that is stored electronically must be treated with the same degree of care as if it were in written form. Unauthorized copying (or copying that MWM determines does not constitute a fair use) of any copyrighted materials, including software, is strictly prohibited. Users must treat confidential and proprietary information belonging to either MWM or a client (including but not limited to financial data, trade secrets, or any other nonpublic information) with the same high level of care required for handling similar material in written form. MWM can supply encryption programs for exchanging confidential communications with clients. All file passwords and codes, including encryption keys, must be disclosed to MWM; no password, code or key that is unknown to MWM can be used.

A violation of this E-mail and Internet Use Policy is a serious breach of MWM's standards of conduct. A person who acts inconsistently with this policy is subject to disciplinary action ranging from revocation of access to the Internet up to and including termination of employment. In some circumstances the person may also be subject to potential civil and/or criminal penalties.

Staff persons who believe that this policy has been or is being violated should immediately notify the Office Manager and/or President.

1. NO PRIVACY RIGHTS

MWM reserves the right and ability to, and periodically will, monitor, review, audit, intercept, access, review and disclose all electronic documents (meaning word processing documents, spreadsheets, databases and computer files of all other kinds) and messages (including E-mail, instant messages, voice-mail and any other means of electronic communications) that are created, received, sent, stored or processed on MWM resources, including such documents and messages which do not relate to MWM's business as well as the World Wide Web sites visited by and browsing history of individual users. Authorized representatives of MWM may and do review such information for any purpose related to MWM business. These purposes may include retrieving business information, trouble-shooting hardware and software problems, preventing system misuse, investigating

misconduct, assuring compliance with software distribution policies and other MWM policies, assuring compliance with applicable legal requirements, and complying with legal and regulatory requests for information.

It is possible that others may access (*i.e.*, view, listen to, copy, print, etc.) electronic documents and messages inadvertently. In addition, even when electronic documents or messages have been "deleted," it may still be possible to retrieve them, and MWM may do so. Further, the use of a password for security does not guarantee confidentiality. The existence of passwords and "delete" function does not restrict or eliminate MWM's ability or right to access electronic communications.

Given these circumstances and business requirements, MWM does not guarantee the privacy of electronic documents and messages stored in MWM-owned or provided files, disks, storage areas or electronic media (even if password-protected). Electronic documents and messages generated or stored on MWM resources are potentially subject to discovery in court cases, can and may be read by others who have the password, and can and may be read by anyone with access to the system if the document or message is neither password-protected nor secured via system access rights.

In using MWM resources, all **Staff persons waive any right to privacy with regard to any use of MWM resources**. MWM resources, including the electronic e-mail system, are MWM property. Messages created, sent, received or stored on MWM premises or using MWM property are and remain the property of MWM. They are not the private property of any Staff person irrespective of any such designation either by the sender or the recipient (including designation as "private," "personal," or "confidential").

Because these communications are not private, Staff persons should be careful in transmitting confidential MWM information. No MWM information should be sent outside MWM unless the recipient is authorized to receive the information.

II. ACCEPTABLE USE POLICY

MWM is committed to protecting the company, its partners and Staff from illegal or damaging actions by individuals, whether intentional or inadvertent.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of MWM. These systems are to be used solely for business purposes in serving the interests of the company, its clients and customers in the course of normal operations.

Violation of these policies may result in disciplinary action, up to and including termination.

A. General Use and Ownership

1. Staff understands and agrees that any data accessed, created or stored on the corporate systems

remains the property of MWM. Because of the need to protect MWM's network, management can and will access information accessed by or stored on any server or electronic device provided by or belonging to MWM.

2. Staff is responsible for exercising good business judgment and discretion regarding personal use. If there is any uncertainty, Staff should consult a supervisor or manager.
3. MWM recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see the Sensitivity Policy..
4. For security, maintenance, or other business purposes, authorized individuals within MWM may access and review equipment, systems, network access or data at any time.
5. MWM reserves the right to audit networks and systems on a periodic basis to ensure compliance with its Electronic Data policies or for any other business purpose.

B. Security and Proprietary Information

1. Information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines. Examples of confidential information include but are not limited to: company private, corporate strategies, proprietary information, competitor sensitive, trade secrets, specifications, customer lists, and research data. Staff should take all necessary steps to prevent unauthorized access to confidential information.
2. Passwords should be kept secure – do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off whenever the point of access is unattended.
4. Confidential and/or proprietary information should be encrypted in compliance with IT Admin group's Acceptable Encryption Use policy.
5. Because information contained on portable devices (laptops, PDAs, etc.) is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.
6. Postings by Staff from a MWM email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of MWM, unless such posting is on behalf of and approved by MWM.
7. All hosts used by Staff connected to the MWM Internet/Intranet/Extranet, whether or not owned by MWM, shall use approved continually executing virus-scanning software with a current virus database.
8. Staff must use extreme caution when opening e-mail attachments or accessing links from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

C. Prohibited Use

1. Illegal activity: Under no circumstances is MWM Staff authorized to engage in any activity that is illegal under local, state, federal or international law.

2. Intellectual Property: Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not licensed for use by MWM.

3. Unauthorized Copying: Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which MWM or the end user does not have an active license is strictly prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a MWM computing asset to actively engage in procuring or transmitting material that could be a violation of sexual harassment policy or create a hostile work environment under federal, state or local law.

8. Making fraudulent offers of products, items, or services originating from any MWM account.

9. Making statements about warranty, expressly or implied, without authorization by MWM.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data to which the Staff person is not an intended recipient or logging into a server or account without authorization. "Disruptions" include, but are not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to IT Admin group is made.

12. Executing any form of network monitoring that can intercept data not intended for the Staff's host without MWM’s authorization.

13. Circumventing user authentication or security of any host, network or account.

14. Interfering with or denying service to any user other than the Staff's host (for example, denial of service attack).

15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

16. Providing information about, or lists of, MWM employees to parties outside MWM.

D. Prohibited Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (spam).
2. Any form of harassment via email, telephone or any other electronic system, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within MWM's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by MWM or connected via MWM's network.
7. Posting any of the above or other non-business-related messages to online groups (spam).

E. Blogging

1. Blogging by Staff, whether using MWM's property and systems or personal electronic devices, is subject to the terms and restrictions set forth in this Policy. Limited and occasional use of MWM's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate MWM's policy, is not detrimental to MWM's best interests, and does not interfere with a Staff person's regular work duties. Blogging from MWM's systems is also subject to monitoring.
2. MWM's Confidential Information policy also applies to blogging. As such, Staff is prohibited from revealing any MWM confidential or proprietary information, trade secrets or any other material covered by MWM's Confidential Information policy when engaged in blogging.
3. Staff shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of MWM and/or any other Staff person.
4. Staff is prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by MWM's Non-Discrimination and Anti-Harassment policy.
5. Staff shall not attribute personal statements, opinions or beliefs to MWM when engaged in blogging. If a Staff person expresses his or her beliefs and/or opinions in blogs, he or she shall not, expressly or implicitly, represent him or herself as an employee or representative of MWM.
6. In addition to following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, MWM's trademarks, logos and any other MWM intellectual property must not be used in connection with any blogging activity

III. Anti-Virus Policy

Viruses can severely impair MWM's ability to conduct business. Staff is therefore required to follow recommended practices to help prevent virus problems.

A. Always run standard, supported anti-virus software available from the network share. Download and

run the current version; install software updates as they become available.

B. NEVER open files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete such attachments immediately and empty Trash.
C. Delete spam, chain, and other junk email without forwarding.
D. Never download files from unknown or suspicious sources.
E. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
F. Back-up critical data and system configurations on a regular basis and store the data in a safe place.

IV. Email Forwarding Policy

To prevent the unauthorized or inadvertent disclosure of sensitive company information, MWM requires adherence to the following email forwarding policy.

Staff is required to exercise utmost caution when sending any email from inside MWM to an outside network.

Absent prior approval by MWM, email will NOT be automatically forwarded to an external destination.

V. Equipment Disposal Policy

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of MWM data, some of which is considered sensitive. In order to protect data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

This policy applies to all technology equipment owned by MWM:

1. When technology equipment has reached the end of its useful life it should be sent to the local Information Technology office for proper disposal.
2. Information Technology will securely erase all storage mediums in accordance with current industry best practices.
3. Equipment which is working, but reached the end of its useful life to MWM, may, at MWM's discretion, be made available for purchase by Staff. Any such purchase is final; no warranty or support

will be provided with any equipment sold.

4. Equipment that is not working or sold will be donated or disposed of according to current environmental guidelines. Information Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.
5. Prior to leaving MWM premises, all equipment must be removed from the Information Technology inventory system.

Failure to properly dispose of technology equipment can result in fines, negative customer perception and costs to notify constituents of data loss or inadvertent disclosure. It is therefore imperative that Staff follow proper disposal techniques.

VI. Password Policy

Password protection is a critical aspect of computer security. Passwords are the front line of protection for user accounts. A poorly chosen password may result in the compromise of MWM's entire corporate network. As such, all Staff is responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

A. General

1. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
2. All production system-level passwords must be part of the IT Admin Group administered global password management database.
3. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
4. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
5. Passwords must not be inserted into email messages or other forms of electronic communication.
6. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
7. All user-level and system-level passwords must conform to the guidelines described below.

B. Guidelines

Passwords are used for various purposes at MWM. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. **NOTE: Do not use either of these examples as passwords!**

B. Password Protection Standards

1. Do not use the same password for MWM accounts as for other non-MWM access (e.g., personal ISP account, option trading, benefits, etc.).

2. Do not share MWM passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential MWM information.

3. **Never, under any circumstances:**
- reveal a password over the phone to ANYONE
- reveal a password in an email message
- reveal a password to the boss
- talk about a password in front of others
- hint at the format of a password (e.g., "my family name")
- reveal a password on questionnaires or security forms
- share a password with family members
- reveal a password to co-workers (for instance, if you are going on vacation)
- use the "Remember Password" feature of applications
- write passwords down or store them in your wallet or office.
- store passwords in a file on ANY computer system, phone or PDA.

If someone requests a password, refer them to this document or have them call someone in the Information Security Department.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to IT Admin Group and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT Admin Group or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions. Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

D. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

VII. Personal Communication Devices and Voicemail Policy

This policy applies to any use of Personal Communication Devices and MWM Voicemail issued by MWM or used for MWM business.

A. **Issuing Policy**

Personal Communication Devices (PCDs) will be issued only to MWM personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCDs are defined to include handheld wireless devices, cellular telephones, laptop wireless cards, pagers and similar devices. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.

Handheld wireless devices may be issued, for operational efficiency, to MWM personnel who need to conduct immediate, critical MWM business. These individuals generally are at the executive and management level. In addition to verbal contact, it is necessary that they have the capability to review and have documented responses to critical issues.

B. Voicemail

Voicemail boxes may be issued to MWM personnel who require a method for others to leave messages when they are not available. Voicemail boxes must be protected by a PIN which must never be the same as the last four digits of the telephone number of the voicemail box.

A. Loss and Theft

Files containing confidential or sensitive data may not be stored in PCDs unless protected by approved encryption. Confidential or sensitive data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the Staff person, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the Staff person. Lost or stolen equipment must immediately be reported.

B. Restriction on Personal Use

PCDs and voicemail are issued for MWM business. Personal use should be limited to minimal and incidental use.

C. PCD Safety—NO DRIVING WHILE USING A PCD

Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If a Staff person must use a PCD while driving, MWM requires the use of hands-free enabling devices.

VIII. Remote Access Policy

To protect against and minimize potential exposure to MWM from damages which may result from unauthorized use of MWM resources, remote access is restricted according to this policy.

This policy applies to all Staff and anyone with a MWM-owned or personally-owned computer or workstation used to connect to the MWM network, and applies to remote access connections used to do work on behalf of MWM, including reading or sending email and viewing intranet web resources.

A. General

1. It is the responsibility of Staff with remote access privileges to MWM's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to MWM.
2. General access to the Internet for recreational use by immediate household members through the MWM Network on personal computers is only permitted for employees that have flat-rate services. The MWM employee is responsible to ensure the family member does not violate any MWM policies, does not perform illegal activities, and does not use the access for outside business interests. The MWM employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of MWM's network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*
4. For additional information regarding MWM's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

B. Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any Staff person provide their login or email password to anyone, not even family members.
3. Staff with remote access privileges must ensure that their MWM-owned or personal computer or workstation, which is remotely connected to MWM's corporate 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.
4. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
5. All hosts that are connected to MWM internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
6. Personal equipment that is used to connect to MWM's networks must meet the requirements of MWM-owned equipment for remote access.
7. Organizations or individuals who wish to implement non-standard Remote Access solutions to the MWM production network must obtain prior approval from Remote Access Services and IT Admin Group.