MANAGEMENT INFORMATION SYSTEMS (MIS)
INTERNET/EMAIL POLICES & PROCEDURES

I. INTRODUCTION

In the past years the MHANATION has made significant investments in information technology. These investments include computers, data communication and the training of many Tribal Employees. In numerous areas of the MHANATION, departments have become reliant and dependent on the use of computer technology to provide effective services to the Tribal membership. Having a large investment in such a critical resource makes it necessary to promulgate policies and standards to guide the organization in effectively managing these resources. Because of the complexities and expenses involved in acquiring and utilizing information technology, policies and standards are needed to insure the security of Tribal information, improve compatibility of systems, provide stability of operations using technology, and minimize cost.

A. Authority

The Tribal Business Council of the Three Affiliated Tribes of the Fort Berthold Indian Reservation pursuant to Resolution #01-05-MWJR, authorizes the Management Information System Department to be responsible for developing all policy and procedures regarding purchasing of computer related equipment.

B. Our Mission

To advance the development and efficient use of Management Information Systems, services and technologies and to increase the effectiveness of the MHANATION and its entities, while safeguarding the information assets of the Tribes.

II. Management Information Systems Office (MIS Department)

The government of the MHANATION is charged with securing and protecting the perpetual health and prosperity of the Tribes. To make this possible, sound decision making by the leadership has a direct relationship to the quality, timeliness and usability of information the leaders have available to them. Therefore, information is recognized as a valuable Tribal asset and resource and should be managed and safeguarded for the current and future generations of the MHANATION.

The management of information via technology in the Tribal organization is like legal advice, accounting and other bodies of knowledge in that is not inherently a "do-it-yourself" prospect. Business people who aren't computer experts rely on professionals to help them plan, manage, and help with technical support. They need to use these people as they use their other professional service suppliers as trusted allies.

III. Department Managers Responsibilities

As computer usages and operational dependency on Information Technology continues to grow it becomes necessary for department managers and supervisors to be directly involved and aware of the use of technology in their departments. All managers and supervisors are required to know Tribal policies and standards and to ensure compliance. Furthermore managers should develop and implement the procedures within their departments.

IV. Business Redemption Plan

Should there be a disaster; each department manager is responsible for recovering critical computer operation in his or her area. The manager may promote readiness and ability to recover from disaster by developing a business redemption plan. The plan should identify key hardware, software and information components of vital systems. It should establish priorities and provide for rapid restoration of the operating system, application programs and data files. See the "Business Redemption Program" section for guidelines in developing this plan.

V. Custodian Responsibilities

Each department manager is custodian of all Tribal property installed in his or her area including computer hardware, software and electronic information. When custodial responsibilities are delegated to others the manager is still responsible for ensuring that procedure for protection and use of these valuable assets are in place and understood. In general, these include:

- Ensuring that proper back up and storage procedures will give sufficient resumption of business and disaster recovery capabilities.

- Assigning security classification to computer systems, electronic information and reports.

- Approving request for information system resources and services.

- Working with MIS to establish and maintain security controls in all stages of planning, development and testing of applications to ensure integrity of programs and electronics information. This applies to systems based on PCs, networks, mainframes and minicomputers.

- Conduct periodic reviews of information systems in order to discover any problems so that plans and budgets can be developed for needed improvements or replacements.

VI. Operational System responsibility

In addition to user management responsibilities listed above each department director or supervisor has a number of operational system responsibilities. They include:

1.) Develop and enforce a back-up program for critical electronic information:

Each computer user in your department should routinely back up their electronic information reports and software programs. Back up is security against data loss and should be done on a consistent basis. Back up media which includes (tapes, cds, optical disks should be clearly labeled to facilitate ease of restoration if necessary. Storing the back-up media away from the computer site provides extra precaution since this reduces the chance of the same event destroying both the original and the backup sets. General guidelines for backing up computers are specified in the section entitled "Back-up and Recovery Procedures."

2.) Maintain a list of all back-ups

It is important to have a list of back up files within a department, so that reports or electronic information can be located without difficulty. This should be routinely maintained, upgraded and stored in a safe place.

3.) Maintain a list of reports produced

So that employees do not re-invent reports which already exist you should maintain a three-ring binder with a master list of all computer reports produced by your department.

4.) Develop an Office Technology Plan.

Department managers are expected to maintain a current Office Technology Plan. This plan supports the budgeting process and includes a list of all computer hardware and software used in their departments. This list of software packages facilitates registration and purchasing upgrades.

VII. Security & Usage Policy

Security controls provide a foundation for the protection of computer based information systems (electronic information, software, equipment and system documentation) from loss, unauthorized use, interruption, modification, disclosure or destruction whether accidental or intentional. These controls include automated security systems, contingency planning and procedures governing proper handling, testing, documentation and use of information systems to safeguard their integrity. If you have any questions regarding the following Tribal Policies pertaining to security, please contact the Management Information Systems (MIS) Department.

A. Tribal Security and Ownership

All systems and electronic information are and shall remain the property of the MHANATION. No part of the computer system or electronic information shall become the private property of any information system user. The MHANATION owns all legal rights to control, transfer, or use all or any part of its systems. All users shall comply with this policy and with all other Tribal policies and rules that apply. Nothing in this policy shall be construed to abridge any rights of the MHANATION to control its systems and their uses or information.

B. Control

The MHANATION reserves and intends to exercise all rights relating to information used in its systems. The MHANATION intends to trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish or withdraw permission for any or all personal or business uses of its systems at any time without cause or explanation. No one shall grant access to Tribal systems without Tribal authorization.

C. Access

Passwords, scramblers, encryption methods or re-mailer services may not be used without Tribal approval, access and control. No user may attempt to access, copy, forward, delete or alter a message of any other user without Tribal authorization. A MHANATION system may not be used to attempt unauthorized access to any information or system.

D. Users shall be lawful and inoffensive

Use of Tribal systems shall not be false, unlawful, offensive or disruptive. No use shall contain profanity, vulgarity, sexual content or character slurs. No use shall make rude or

hostile references to race, age, gender, sexual orientation, religious or political beliefs, national origin, health or disability. Copyrighted or licensed information shall be used only with full legal right to do so.

VIII. Personal use restricted

The MHANATION often requires people to remain at work despite personal needs and interests. The MHANATION also needs employees to continuously develop their knowledge and skills. For those reasons, certain personal uses are allowed. The MHANATION shall have sole discretion to decide whether a use is personal or business. Any personal use shall satisfy the following provisions. Except as this provision clearly states all personal use shall also comply with the rest of this policy.

1.) Personal use shall be done outside the employee's normal working hours.

2.) Personal use of Tribal systems shall be at virtually no cost to the Tribe.

3.) The degree or extent of personal use shall always be insignificant compared to use for assigned work.

4.) No personal use may be made by or on behalf of any other organization or third party.

5.) No publishing is allowed if the purpose is personal. This bars personal posting to Internet groups, chat rooms, web pages or list services.

6.) No soliciting is allowed. System may not be used to lobby, solicit, recruit, sell or persuade for or against commercial ventures, products, religious or political cause outside the organization or the like.

7.) A user may not put to his or her personal use any system devices that the user does not employ in his or her assigned work. No privately owned device may be connected to the MHANATION system without Tribal authorization. System devices taken home remain subject to this policy.

8.) Employees may make limited personal use of their assigned computers, software and internet access. Uses include web searches for personal research, self-study and preparing a resume for application for a Tribal Job.

9.) Users may not install or download software without Tribal authorization. This includes music/file sharing programs.

10.) Computer games, internet games and personal games may not be used. Games that come with software are to be deactivated and not used. Software games that teach real needed knowledge or skills may be used with Tribal authorization.

IX. Securing Tribal Owned Computer Resources

All computer equipment, peripherals, software programs, electronic information and computer generated reports are assets of the MHANATION and shall be protected from misuse, unauthorized manipulation and destruction. Protection measures may be physical and or software based.

X. Computer Resources Custodial Requirements

All computer assets are assigned to a responsible party. Each application system, its associated equipment, software programs and electronic information are assigned to a custodian who is responsible for ensuring that adequate controls and procedures are in place to protect the integrity of the resources. Procedures include the disposal of reports, design and testing of applications and general usage.

The department director/supervisor is the custodian and may delegate another person to authorize access to these resources as custodian, but will remain ultimately responsible for their protection.

XI. Security Administration

It is the duty of every employee to observe security and report violations to the department director or person delegated as custodian of information systems resources within the department.

XII. User Access to Management Information Systems

1) All users are held accountable for all action performed on the information systems with their login ID (i.e., user name and password).

2) Users are only to perform functions on the computer systems for which they are authorized and in direct support of their job function.

3) All access to information systems resources permitted to users shall have the approval of the supervisors.

XIII. Password Administration

Password security is used to prevent unauthorized access to information stored on the computer or the network and to prevent the loss or destruction of that information and related equipment. Computers and the network are often used to store sensitive, private and confidential information which must be carefully guarded against unauthorized access. Directors and supervisors shall give access to such information based on need to know and a clearance process. Examples are Tribal Court, Social Services and Finance, etc.

All entry points into the Tribal Network, file server or shared computer(s) shall employ passwords as the authentication technique. The following policies for the use of authentication passwords on Tribal System shall be followed.

1) Passwords and network IDs shall not be shared under any circumstance. Disclosure of a password and or network ID is a serious security violation and may result in loss of system access privileges and possible disciplinary actions. Users are often tempted to share Login IDs and passwords when working together on projects that require sharing computer documents and electronic information. However these sharing requirements are easily met with separate Login Ids and passwords.

2) Passwords are not to be saved by computer software in a way that lets you log into the network or central computer without entering your password.

3) Passwords should be changed every 30-50 days or when requested by the MIS Department.

4) When unattended during the workday or outside of office hours, personal computers are to be secured against unauthorized access. You can accomplish this either by logging out of the network, shutting the computer down, locking your office door or by activating password protection on the individual computer. If you use a Power-on password for your PC, you will need to share the password with your supervisor and or MIS Department. This is done in order to permit other authorized personnel to use or to service your PC when you are away for an extending time.

XIV. Contingency Planning-Back-up Recovery

Department directors/supervisors should ensure that recovery procedures are in place so that all critical application systems and electronic information are recoverable without seriously hampering Tribal Operations. Department directors/supervisors are responsible for ensuring that procedures and resources are available to carry on business in an emergency.

XV. Hardware

All New equipment shall be registered with the Management Information Systems Department and with Property and Supply for inventory and warranty control purposes. Treat your computer as you would any piece of delicate equipment that you depend on. Know the model, serial number and key characteristics of your equipment.

1.) Personal computers and peripherals are not to be used unless authorized by the Manager/Supervisor. Copies of the authorization to use personal equipment shall be filed with the Management Information System Department.

2.) Do not allow machines and other sensitive items such as diskettes or USB drives to be exposed to elements such as dust, smoke etc. which can easily harm the electronic circuitry.

3.) Only staff authorized by the MIS Director shall repair or install equipment.

4.) All computers and communications equipment shall be plugged into authorized surge protectors or UPS units.

5.) Hardware purchased with Tribal funds or with funds administered by the Tribes shall be registered with vendors under the corporate name "Three Affiliated Tribes" and this name only. Personal names shall not be used as the hardware and their related warranties are the property and responsibility of the Tribes.

XVI. Software

1.) Software purchased with Tribal funds or with funds administered by the Tribes shall be registered with vendor under the corporate name "Three Affiliated Tribes" and this name only. Personal names shall not be used, as the software is the property and responsibility of the MHANATION.

2.) Privately owned software registered to the individual shall not be loaded on Tribal Computers.

3.) Under no circumstances shall unregistered or unlicensed software be loaded or used on a tribal computer, unless it is legally recognized shareware or public domain software.

4.) Purchased software is a valuable Tribal asset. The software's original diskettes/CDs and documentation shall be kept in a safe, secure place. You should avoid loaning the original or back-up diskettes/CDs or packaged software to other personnel, as unauthorized use of the software may violate copyright laws, regulations, Tribal policies or procedures.

5.) It is the responsibility of the individual department managers and supervisors to insure that their employees do not violate any license or copyright laws, regulations, tribal policies or procedures.

Software is copyright protected in the same manner as other media such as records, books and film. The fact that software is so easy to copy does not legitimize its duplication. Unless a site license had been acquired, offices are expected to purchase and track the requisite number of licenses and use all commercial software in

accordance with licensing agreements. If unlicensed software is discovered on a computer it shall be immediately purchased or removed.

Tribal policy requires that all computer users adhere to vendor restrictions placed on the use of computer and office hardware and software. Such restrictions prohibit duplication of software and its documentation, whether for in-house or for personal use. Any questions regarding interpretation of this issue should be directed to the Management Information System Department for clarification.

Each software Application has its individual copyright policy governed by the manufacturer. It is imperative that you follow and adhere to these restrictions for legal reasons; copyright restrictions can be located in the documentation accompanying each software package.

UNDER NO CIRCUMSTANCES WILL COPYRIGHTED SOFTWARE OR DOCUMENATION BE COPIED FOR USE ON ANOTHER TRIBAL COMPUTER OR ON PERSONALLY OWNED COMPUTERS.

XVII. Email Security Policy

A. Purpose

This section provides specific instructions on the ways to secure electronic mail (e-mail) resident on personal computers and servers.

B. Scope

The policies apply to all Tribal employees and Entities and cover e-mail located on MHANATION personal computers and servers if these systems are under the jurisdiction and/or ownership of the MHANATION. The policies apply to stand-alone personal computers with dial-up modems as well as those attached to networks.

C. Company property

As a productivity enhancement tool, the MHANATION encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of the MHANATION, and are not the property of users of the electronic communications services.

D. Authorized usage

The MHANATION electronic communications system generally must be used only for business activities. Incidental personal use is permissible so long as:

1.) Does not consume more than a trivial amount of resources.
2.) Does not interfere with staff productivity (including chain emails).
3.) Does not preempt any business activity (including chain emails).

Users are forbidden from using the MHANATION electronic communication system for charitable endeavors, private business activities, or amusement/entertainment purposes (i.e. lunch sales, bingo announcements) unless expressly approved by the MHANATION Chairman or Councilmen. Users are also forbidden from sending mass emails or chain emails not pertaining to work-related issues. This includes but is not limited to good luck emails, money-making schemes, and chain emails which include pictures, which take up bandwidth reserved for Tribal use. Employees are reminded that the use of Tribal resources, including communications, should never create either the appearance or the reality of inappropriate use.

E. Default privileges

Employee privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of "need-to-know." For example, end users must not be able to reprogram electronic mail system software. With the exception of emergencies and regular system

maintenance notices, broadcast facilities must be used only after the permission of a program director has been obtained.

F. User separation

These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user IDs and associated passwords to isolate the communications of different users. All MHANATION staff and authorized entities must have unique usernames and passwords to access the e-mail system.

G. User accountability

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. In doing so exposes the authorized user to be held responsible for actions the other party takes with the password. If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities).

H. No default protection

Employees are reminded that the MHANATION electronic communications system is not encrypted by default. If sensitive information must be sent by e-mail, encryption or similar technologies to protect the data must be employed. See the Management Information Systems Department if this requirement is needed.

I. Respecting privacy rights

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing electronic communications. The MHANATION is committed to respecting the rights of its employees, including their reasonable expectation of privacy. However, the MHANATION also is responsible for servicing and protecting its electronic communications networks. To accomplish this, under different circumstances, it is necessary to intercept or disclose, or assist in intercepting or disclosing electronic communications.

J. No guaranteed message privacy

The MHANATION cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

J. Regular message monitoring

It is the policy of the MHANATION to NOT regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that the MHANATION will from time to time examine the content of electronic communications.

K. Statistical Data

Consistent with generally accepted business practice, the MHANATION collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. using such information, Management Information Systems staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

L. Incidental disclosure

It may be necessary for MIS staff to review the content of individual employee's communications during the course of problem resolution. MIS staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels (program director, Chairman, etc.).

M. Message forwarding

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. MHANATION sensitive information must not be forwarded to any party outside the MHANATION without prior approval of a program director or the TAT Council. Blanket forwarding of messages to parties outside the MHANATION is prohibited unless the prior permission of the programs manager has been obtained.

N. Purging electronic messages

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After a certain period-generally six months-electronic messages backed up to a separate data storage media (tape, disk, CD-ROM, etc.) will be automatically deleted by MIS staff. Not only will this increase storage space, it will also simplify record management and related activities. If the MHANATION is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the MHANATION Council or designated representative communicated that it is legal to do so.

O. Responsibilities

As defined below, the MHANATION groups and staff members responsible for electronic mail securities have been designated in order to establish a clear line of authority and responsibility.

1) Management Information Systems must establish e-mail security policies and standards and provide guidance on e-mail security to all MHANATION staff.

2) MIS staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Program directors must ensure that their staffs are in compliance with the personal computer security policy established in this document. MIS staff must also provide administrative support and technical guidance to management on matters related to e-mail security.

3) MHANATION program directors must ensure that:

    - Employees under their supervision implement e-mail security measures as defined in this document

P. Contact point

Questions about this policy may be directed to the Management Information Systems department.

Q. Disciplinary process

Violation of these policies may subject employees to disciplinary procedures up to and including termination.