Information Technology Department (ITD) Fort Peck Assiniboine & Sioux Tribes Policy for Personal Use of IT Resources

Revised July 2024

Introduction

The purpose of this document is to establish policy regarding personal use of Information Technology (IT) Resources within the Fort Peck Tribes (FPT).

The guidelines contained in this Tribal document apply to all Tribal departments and programs utilizing the FPT IT Resources, network telecommunications, Local-Area-Networks (LANs) and Wide-Area-Network (WANs), including the personnel, equipment, procedures, and technologies that are employed in managing these activities.

The Information Technology Department will develop the guidelines and/or policies for use of Information Technology Resources; maintain established guidelines and policies; develop the criteria for use of Information Technology Resources; and manage and oversee the overall operations of the FPT Network, Hardware, Software, and IT Resources. The Tribal Chairman and Council will be the final authority within the Tribe to resolve any conflicts over use of Tribal IT resources.

Table of Contents

Purpose

The purpose of this Fort Peck Tribes (FPT) document is to convey this policy for limited acceptable personal use of FPT information technology (IT) resources to employees, contractors, interns and other FPT personnel. This policy has established privileges and responsibilities for employees of the FPT. It recognizes these employees as responsible individuals who are the key to making the Tribes and Tribal Programs more responsive to its members. It allows employees to use FPT IT resources for non-tribal purposes when such use involves minimal additional expense to the tribe, is performed on the employee's non-work time, does not interfere with the mission or operations of the FPT, and does not violate ethical conduct or other FPT policies and procedures.

Background

The Fort Peck Tribal Council serves the enrolled members on the Fort Peck Assiniboine and Sioux Reservation. Increasingly, the Council is called upon to deliver more and better services to a growing population that continues to expect ever-increasing improvements in service delivery. Much of this productivity increase has come about using modern information technology such as computers, facsimile machines, and the Internet. FPT employees shall be provided with a professional supportive work environment. They shall be given the tools needed to effectively fulfill their assigned responsibilities. Allowing limited personal use of these tools helps enhance the quality of the workplace and helps the Tribes to retain highly qualified and skilled workers.

Scope

This policy applies to all Tribal employees and Tribal Programs, including organizations conducting business for and on behalf of the Tribe through contractual relationships when using FPT IT resources. The policies contained in this FPT document apply to all FPT IT activities including the equipment, procedures and technologies that are employed in managing these activities. The policy includes teleworking, travel, and other off-site locations as well as all the office locations of the FPT. This policy does not supersede any other applicable law or higher-level agency directive or policy guidance. Tribal Program Directors shall apply this policy to contractor personnel, interns, and other non-tribal employees through incorporation by reference in contracts or memorandums of agreement as conditions for using Tribes provided IT resources.

Policy

The following policies shall be in effect for each Tribal Department/Program unless the Tribal Department/Program adopts a more restrictive set of personal use policies preclude one or more of the policies listed below.

Employees are permitted limited personal use of FPT IT resources. This personal use shall not result in loss of employee productivity, interference with official duties or other than "minimal additional expense" to FPT in areas such as:

- communications costs for voice, data, or video image transmission.
- use of consumables in limited amounts (such as: paper, ink, toner).
- general wear and tear on equipment.
- data storage on storage devices.
- transmission impacts with moderate e-mail message sizes, such as emails with small attachments.

Employees have no inherent right to employ FPT IT resources for personal use.

Unauthorized or inappropriate use of FPT IT resources could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, criminal penalties and/or employees or other users being held financially liable for the cost of inappropriate use.

Employees are expected to conduct themselves professionally in the workplace and to refrain from using Tribal office equipment for activities that are inappropriate. Misuse or inappropriate personal use of FPT IT resources includes:

- any personal use that could cause congestion, delay, or disruption of service to any FPT IT resource. For example, video, sound, or other large file attachments can degrade the performance of the entire network as do some uses of "push" technology, such as audio and video streaming from the Internet.
- the intentional creation, downloading, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials.
- the intentional creation, downloading, viewing, storage, copying or transmission of materials related to illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.
- use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (such as consulting for pay, sales or administration of business transactions, sale of goods or services).
- posting Tribal or personal information to external newsgroups, bulletin boards or other public forums without authority, including information which is at odds with Tribal missions or positions. This includes any use that could create the perception that the communication was made in one's official capacity as a Tribal employee unless appropriate approval has been obtained.
- establishing personal, commercial, and/or non-profit organizational

web pages on Tribe owned machines.

- use of FPT systems as a staging ground or platform to gain unauthorized access to other systems.
- the creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- use of FPT IT resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to hate speech, or material that ridicules others based on race, creed, religion, color, age, sex, disability, national origin, or sexual orientation.
- the addition of personal IT resources to existing FPT IT resources without the appropriate management authorization, including the installation of equipment on FPT data lines and reconfiguration of systems.
- use that could generate more than minimal additional expense to the Tribes.
- the intentional unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data.
- use or creation of unauthorized list servers or the distribution of unauthorized newsletters.
- using another person's digital authentication.
- sending anonymous messages.
- avoiding established security procedures.
- using Peer-to-Peer (P2P) software without IT Director (or designee) approval.

Department/Program Supervisors/Directors may adopt policies that are more restrictive than those contained in this Tribal policy.

Any use of FPT IT resources, including e-mail, is made with the understanding that such use may not be secure, is not private, and is not anonymous and may be subject to disclosure under the Freedom of Information Act (FOIA).

FPT employees do not have a right to, nor shall they have an expectation of, privacy while using FPT IT resources at any time, including accessing the Internet through FPT gateways and using email, which may be subject to release pursuant to the Freedom of Information Act. To the extent that employees wish that their private activities remain private, they shall avoid making personal use of FPT IT resources.

Electronic data communications may be disclosed within individual Programs to employees who have a need to know in the performance of their duties (such as, with manager approval technical staff may retrieve e-mail or documents from a user's

computer). The privacy rights of an individual may not be violated.

Roles and Responsibilities

The Information Technology Department

Information Technology Department is responsible for:

- the dissemination of this policy to all employees within their respective organizations.
- training all employees on personal use policies and to include inappropriate use.
- implementing security controls to prevent and detect improper file sharing.
- establishing waiver procedures and signature file for any and all approved Peer-to-Peer software purchases and implementations.
- informing users of their rights and responsibilities, including the dissemination of the information in this policy to individual users.
- notifying, when appropriate, law enforcement officials.

Department/Program Supervisors/Directors

Department/Program Supervisors/Directors, in their supervisory role, are responsible for:

- addressing inappropriate use by employees who report to them.
- receiving reports of inappropriate use from the IT Department and sharing these reports, as appropriate, within their own management structure.
- Managers of FPT IT Resources may use system monitoring software in order to improve the performance of the resource. When a Program Director identifies an inappropriate use, he/she shall notify the IT Department and, as appropriate, terminate the access of the individual(s) to the IT resource after informing the IT Department of the action to be taken.

FPT Employees and Users of FPT IT Resources

Users, including employees, contractors, interns, and others, when using IT equipment that FPT uses in official capacity, are responsible for:

- seeking guidance from their supervisors when in doubt about the implementation of this policy.
- ensuring that they are not giving the false impression that

they are acting in an official capacity when they are using FPT IT resources for non-tribal purposes. If there is expectation that such a personal use could be interpreted to represent the Tribes or Tribal Program, then an adequate disclaimer shall be used. For example:

"The contents of this message are mine personally and cannot be construed to be endorsed (inferred or implied) neither by the Tribes nor Tribal Program."

- following policies and procedures in their use of IT Resources (for example: Internet and e-mail) and refraining from any practices which might jeopardize FPT computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet.
- learning about Internet etiquette, customs, and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.
- familiarizing themselves with any unique requirements for accessing, protecting, and utilizing data, including Privacy Act requirements, copyright requirements.
- adhering to all conditions set forth in this and other Tribal Policies.
- completing IT security training on Tribal personal use policies. Policies include a waiver or exception process.

FPT employees may use FPT IT resources for authorized purposes only. Limited personal use of Tribal office equipment by employees during non-work time is considered to be an "authorized use" of Tribal property.

Risk Management

Risk management refers to the process of identifying risk, assessing risk, and taking the necessary steps to reduce risk to an acceptable level. A risk management program is an essential management function and is critical for the tribes to successfully implement and maintain an acceptable level of security. A risk management process must be implemented to assess risk to the Fort Peck Tribes IT systems.

As a part of a risk-based approach used to determine sufficient security for its IT property, the Tribes shall implement a process to assess the acceptable risk to the Tribes IT assets. The IT department shall analyze threats and vulnerabilities and select appropriate, cost-effective controls to achieve and maintain an acceptable level of risk.

In the event an identified risk cannot be fully remediated, mitigation steps must be taken to reduce the risk. The risk and steps taken to mitigate the risk must be formally

documented, accepted, and approved by the Fort Peck Tribes Chief Technology Officer. All risk acceptances will be reviewed annually or until the identified risk no longer exists.

Data Breach

If (or when) electronic records are breached and Personal Identifiable Information (PII) is disclosed outside of the Fort Peck Tribes, programs and providers must have a data breach response plan in place to adhere to applicable federal laws, while also protecting the privacy and confidentiality of those whose PII was disclosed. Programs will need to inform individuals that their information was disclosed so they can take steps to protect against any potential fallout of that disclosure. Programs will also need to think through how to safely contact individuals to inform them of the data breach.

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses positive and unlabeled data (PU) by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PU and portable electronic storage media that store PU, the inadvertent disclosure of PU on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PU for other than authorized purposes. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PU, as is often the case with a lost or stolen laptop or electronic storage device.

Some common examples of a breach include:

- A laptop or portable storage device storing PU is lost or stolen.
- An email containing PU is inadvertently sent to the wrong person.
- A box of documents with PU is lost or stolen during shipping.
- An unauthorized third party overhears department employees discussing PII about an individual seeking employment or benefits; A user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual.
- An IT system that maintains PII is accessed by a malicious actor; or
- PII that should not be widely disseminated is posted inadvertently on a public website.

Procedures in the event of a Breach Incident.

1. The FPT IT Department, department supervisors/immediate supervisors and the department Director/Administrator will meet in the event of a data or security breach. This team will consist of the FPT Chief Technology Officer, FPT IT Department, Department supervisor or immediate supervisor, and the department Director/Administrator. In the event of a breach, the individuals listed shall meet at a designated location. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach, or exposure has occurred. They will determine the severity of the situation and will cooperatively decide which set of procedures to follow based on the type of incident and information available at that time.

2. These standard operating procedures will be utilized by all departments operating under the Fort Peck Tribes in the event of a data or security breach situation. Paramount is the retention and safe keeping of confidential information.

3. This applies to all Fort Peck Tribes personnel in cooperation with the Data Breach Response Team.

4. This policy mandates that any individual who suspects that a theft, breach, or exposure of protected or sensitive data has occurred, must immediately provide a description of what occurred by calling their immediate supervisor and that supervisor notifying the following individuals listed above.

5. Departments of the Fort Peck Tribes must inform the FPT Chief Technology Officer of all emergency events.

6. The following procedure is intended to provide guidance and direction in determining how the FPT will respond when a data breach or security breach is discovered.

Step 1. <u>Supervisors or Immediate Supervisors</u>

A. Notify the department's supervisor or immediate supervisor in the event of notification of a data breach from the department personnel.

B. Determine whether a true breach has occurred and its potential impact.

C. Identify the nature, scope, impact and origin or root cause of the breach.

D. Remove all access to the workstation or server to prevent confidential information from being exported from workstations or servers.

E. Collect evidence regarding the breach.

Step 2. FPT Chief Technology Officer

A. Assist in detecting how security was breached.

B. Assist in collecting evidence regarding the breach.

C. Assist in responding to ongoing threats.

D. Recommend security procedures and enhancements

Step 3. FPT Directors

A. Provide clear and immediate communication about what happened, and steps staff should take.

B. If necessary, develop messaging and deployment schedule for notifying those whose data was compromised based on legal counsel

C. Provide any necessary disciplinary actions for failure to comply with Fort Peck Tribes Policies.

Step 4. FPT Chief Technology Officer

A. Draft a report. This report will include
   a. Date of incident
   b. Location of incident
   c. Systems affected
   d. Method of detection
   e. Nature of incident
   f. Description of incident
   g. Actions taken/resolution

B. Educate staff on data breach and security threat prevention.

C. In severe cases, where criminal activity was determined as a root cause of the breach, the FPT Chief Technology Officer shall forward a completed incident report to the proper chain of command for further reporting to law enforcement, Human Resources, Tribal Executive Board, etc.

Project Planning

FPT IT projects, including system development, enhancement, maintenance, and infrastructure activities shall be managed to ensure that delivered solutions are consistent with this policy.

Plans for executing IT projects should include a general process for addressing IT security controls. The FPT shall ensure that all major IT development or infrastructure projects have a corresponding project plan that address the security control requirements within this policy. The FPT Information Security shall be a part of this planning process.

Operational Level Controls

Security Education and Awareness

The FPT Department Directors and Supervisors are responsible for educating users on security threats that may impact secure operations of the FPT Information Technology network and provide information on mechanisms to protect against these threats. The FPT must ensure all active users regularly participate in a formal security education and awareness training program. The program must have the ability to track completion of required security training assignments and report on non-compliance. The formal program must also include learning opportunities for users to independently explore information on safe computing practices.

Configuration Management

System hardening procedures shall be created and maintained to ensure up to date security leading practices and deployed for all IT operating systems, applications, databases, network, and hardware devices. All default system administrator passwords must be changed. The FPT shall implement an appropriate change management process to ensure changes to systems are controlled by:

- Developing, documenting, and maintaining current baseline configurations.
- Network devices, host operating systems, and databases must be patched and updated for all security related updates/patches using automated tools when possible.
- Baseline images for servers and workstations must be established and reviewed annually.
- Developing, documenting, and maintaining current inventories of the components of information systems and relevant ownership information.
- Configuring the security settings of information technology products to the most restrictive mode consistent with operational requirements.

- Analyzing potential security impacts of changes prior to implementation.
- Authorizing, documenting, and controlling system level changes.
- Restricting access to system configuration settings and provide the least functionality necessary.
- Prohibiting the use of functions, ports, protocols, and services not required to perform essential capabilities for receiving, processing, storing, or transmitting confidential information.
- Maintaining backup copies of hardened system configurations.

Network Connection Management

With the exception of the FPT provided connections, external network connections shall be permitted only after all approvals are obtained consistent with this policy and shall be managed as agreed to by the FPT and the untrusted entity. These connections are subject to the policies of the FPT and should not be part of the ordinary process of doing business. Specific criteria should be included in the system that includes:

- Purpose and duration of the connection as stated in the agreement, lease, or contract.
- Points of contact and cognizant officials for both the FPT and untrusted entities.
- Roles and responsibilities of points of contact and cognizant officials for both FPT and untrusted entities.
- Security measures to be implemented by the untrusted organization to protect the FPT IT properties against unauthorized use or exploitation of the external network connection.
- Controls to detect and monitor for the connection of unauthorized devices to the FPT IT system.
- Requirements for notifying the FPT Chief Technology Officer within two business days of a security incident on the network.

Disaster Preparedness Plan

The FPT shall develop, implement, and test an IT Disaster Preparedness plan for all Information Systems determined to be essential for ongoing business. Creation, maintenance, and annual testing of a plan will minimize the impact of interruptions of information technology service delivery caused by events ranging from a single disruption of a business to a disaster. Disaster Preparedness Plan Maintenance should be incorporated into the Management Information Systems (MIS) architecture review and change management processes to ensure plans are kept current.

Primary components of an IT Disaster Preparedness Plan are:

- Identification of a disaster preparedness team
- Definitions of preparedness team member responsibilities
- Documentation of each critical system including:
    - Purpose
    - Hardware
    - Operating System
    - Business and middleware application(s)
    - Data
    - Supporting network infrastructure and communications
- System restoration priority and dependency list
- Description of back-up storage location
- Description of back-up testing procedures (including frequency)
- Identification of alternate site including contact information
- System Recovery Time Objective RTO (time between unexpected failure to normal operations)
- System recovery Point Objective RPO (how current the data should be at RTO)
- Procedures for information technology service delivery at alternate and primary production MIS site.

Incident Management

Incident management refers to the processes and procedures the Chief IT Technology Officer implements for identifying, responding to, documenting, and managing information security incidents. A security incident within the FPT managed networks is defined as a violation of the Fort Peck Tribes Personnel, IT Department policies, acceptable use policies, or standard computer security practices.

Things to keep in mind:

User ID's and passwords will be assigned to all users. Tribal employees/contractors may use passwords only in the performance of their official duties.

Employees/contractors may not disclose any User ID's and passwords to anyone for any reason.

Employees/contractors will be held accountable for all work performed on or changes made to the system/databases under their User ID's and passwords.

Employees/contractors will not allow anyone else to access any of the above designated computer systems, or through them, to any other computer system, using their User ID's and passwords.

Information and Assistance

Direct questions, comments, suggestions, or requests for further information to the IT Department at itd@fortpecktribes.net

Glossary

- Browser - a software tool used to locate and view data in standardized formats on other computers.
- Employee – any person (includes interns, contractors, visitors, and state, local or government program participants), company or service provider who performs work, tasks, duties for or at the direction of FPT.
- Employee non-work time - times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use Tribal office equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).
- FPT Information Technology resources - includes but is not limited to personal computers and related peripheral equipment and software, network and web servers, telephones, facsimile machines, photocopiers, Internet connectivity and access to internet services, email and, for the purposes of this policy, office supplies. It includes data stored in or transported by such resources for FPT purposes.
- Information Technology (IT) - any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data.
- Internet - a worldwide electronic system of computer networks which provides communications and resource sharing services to Tribal employees, businesses, researchers, scholars, librarians, and students as well as the general public
- Minimal additional expense - the employee's personal use of FPT IT resources is limited to those situations where the Tribe is already providing equipment or services and the employee's use of such equipment or services shall not result in any additional expense to the Tribes or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner or paper. Examples of minimal additional expenses include making a few photocopies, using a computer printer to printout a few pages of material, making occasional brief personal phone calls, infrequently sending personal email messages, or limited use of the Internet for personal reasons.

- Peer-to-Peer (P2P) file sharing – is defined as: "…any software or system allowing individual users of the Internet to connect to each other and trade files. While there are many appropriate uses of this technology, the majority of files traded on P2P networks are copyrighted music files and pornography. P2P is a common avenue for the spread of computer viruses within IT systems".
- Personal use - activity that is conducted for purposes other than accomplishing official or Tribal business. FPT employees are specifically prohibited from using Tribal office equipment to maintain or support a personal private business. Examples of this prohibition include employees using a Tribal computer and Internet connection to run a travel business or investment service. Using Tribal office equipment to support a personal private business is prohibited. Employees may, however, make limited use under this policy of Tribal office equipment to, for example but not limited to, check their 401(k) or other personal investments, or to seek employment, or communicate with a volunteer charity organization.
- Privilege - in the context of this policy, that FPT is extending the opportunity to its employees to use FPT IT resources for personal use in an effort to create a more supportive work environment. However, this policy does not create the right to use FPT IT resources for nontribal purposes. Nor does the privilege extend to modifying such equipment, including loading personal software, or making configuration changes.
- Shared FPT IT resource - any FPT IT resource that is managed by one FPT Program but used by more than one employee (such as, the Finance software).
- Teleworking - teleworking, also known as telecommuting, means you work from home or a satellite office near your home. You stay in touch with your office by telephone, FAX, network connection or email. Some employees telework one day a week or more, depending on their employer.
- World-Wide Web (WWW) - The collection of web pages (documents) which are developed in accordance with the HTML (hypertext) Web format standard and may be accessed via Internet connections using a web browser, such as Microsoft Edge, Google Chrome, or Mozilla's Firefox.

Fort Peck Assiniboine and Sioux Tribes Personal Use of IT Resources Acceptance

PRIVACY EXPECTATIONS. Any use of Fort Peck Tribes (FPT) IT resources, **including email**, is made with the understanding that such use may not be secure, is not private, is not anonymous, and may be subject to disclosure under the FOIA. Employees do not have a right to, nor shall they have an expectation of, privacy while using FPT IT resources at any time, including accessing the Internet through the FPT Network and **using e-mail**, which may be subject to release pursuant to the FOIA. To the extent that employees wish their private activities to remain private, they shall avoid making personal use of FPT IT resources.

IMPLIED CONSENT. Employees imply their consent to disclose the contents of any file(s) or information maintained or passed through FPT IT resources. By using FPT IT resources, consent to monitoring and recording is implied with or without cause, including but not limited to accessing the Internet and **using e-mail**.

MONITORING TOOLS. The FPT system managers and supervisors may access any electronic communications and employ monitoring tools to detect improper use. Electronic communications may be disclosed within the FPT to employees who have a need to know in the performance of their duties (e.g., with manager approval, technical staff may employ monitoring tools in order to maximize the use of their resources, which may include the detection of inappropriate use).

PENALTIES. Unauthorized or improper use of FPT IT resources could result in the loss of use or limitations on the use of FPT IT resources, disciplinary or adverse actions, criminal penalties, and/or employees being held financially liable for the cost of improper use.

I _____, understand, will abide by, and agree to
Print Name
the above stated Acceptance concerning the Personal Use of IT Resources. This Acceptance is taken from the “Fort Peck Tribes Policy on Personal Use of Information Technology Resources,” and the “Fort Peck Tribes Policy on Internet and E-Mail.”

Employee Signature_____

Employee Title_____

Date_____

Department/Program_____

RESOLUTION #32-717-2024-07 **TRIBAL GOVERNMENT FINANCE**

WHEREAS, the Fort Peck Tribal Executive Board is the duly elected body representing the Assiniboine and Sioux Tribes of the Fort Peck Reservation and is empowered to act on behalf of the Tribes. All actions shall be adherent to provisions set forth in the 1960 Constitution and by-laws; and

WHEREAS, the *Information Technology Department (ITD) Fort Peck Assiniboine & Sioux Tribes Policy for Personal Use of IT Resources* is currently outdated and lacks a section of a proper procedure and response in the event of a data breach; and

WHEREAS, it is recommended that the Fort Peck Tribes Information Technology Department add a risk management section to the *Information Technology Department (ITD) Fort Peck Assiniboine & Sioux Tribes Policy for Personal Use of IT Resources* and update the glossary to reflect the current amendment.

NOW THEREFORE BE IT RESOLVED, The Tribal Executive Board hereby approves and authorizes the Information Technology Department to update the *Information Technology Department (ITD) Fort Peck Assiniboine & Sioux Tribes Policy for Personal Use of IT Resources* to establish a proper policy in the event of a data breach.

CERTIFICATION

I, the undersigned Secretary/Accountant of the Tribal Executive Board of the Assiniboine and Sioux Tribes of the Fort Peck Indian Reservation, hereby certify that the Tribal Executive Board is composed of 12 voting members of whom 11 constituting a quorum were present at a Special Board meeting duly convened this 8th day of July, 2024 and that the foregoing resolution was duly adopted at such meeting by the affirmative vote of 9 for, 0 opposed, 2 not voting, and 1 absent.

Secretary Accountant/Secretary

APPROVED:

Chairman/Vice Chairman
Fort Peck Tribal Executive Board