



# United States Department of the Interior

OFFICE OF THE SECRETARY

Washington, DC 20240

**JUN 08 2023**

The Honorable Glen Nenema  
Chairman, Kalispel Indian Community  
of the Kalispel Reservation  
P.O. Box 39  
Usk, Washington 99180

Dear Chairman Nenema:

On April 27, 2023, the Kalispel Indian Community of the Kalispel Reservation (Tribe) and the State of Washington (State) submitted the Memorandum of Incorporation of Most Favored Nation Amendments to the Tribal-State Compact for Class III Gaming between the Kalispel Tribe of Indians (Tribe) and the State of Washington (Amendment), providing for the regulation of class III gaming activities by the Tribe. The Amendment replaces Section III(O) with language to clearly establish which individuals will be allowed to carry firearms within the gaming facility, such as law enforcement, or other individuals authorized by the Tribe's ordinances and that the Tribe will maintain a list of all authorized persons. It also adds language regarding tort liability for negligent use of firearms. The Amendment adds Appendix T, Technical Requirements Governing the Gaming Data Environment and adds Appendix W, Rules Governing Wide Area Progressives.

We have completed our review of the Amendment and conclude that it does not violate the Indian Gaming Regulatory Act (IGRA), any other provision of Federal law that does not relate to jurisdiction over gaming on Indian lands, or the trust obligations of the United States to Indians. 25 U.S.C. § 2710(d)(8)(B). Therefore, pursuant to my delegated authority and Section 11 of IGRA, I approve the Amendment, 25 U.S.C. § 2710(d)(8)(A). The Amendment takes effect when the notice of this approval is published in the *Federal Register*. 25 U.S.C. § 2710(d)(3)(B).

A similar letter is being sent to the Honorable Jay Inslee, Governor, State of Washington.

Sincerely,

Bryan Newland  
Assistant Secretary - Indian Affairs

Enclosure

**MEMORANDUM OF INCORPORATION**  
**of**  
**MOST FAVORED NATION AMENDMENTS**  
**To The**  
**TRIBAL-STATE COMPACT FOR CLASS III GAMING**  
**Between the**  
**KALISPEL TRIBE OF INDIANS**  
**and the**  
**STATE OF WASHINGTON**

The Kalispel Tribe of Indians (“Tribe”) and the State of Washington (“State”) entered into a Tribal-State Compact for Class III Gaming (“Compact”) on October 22, 1998, which was amended five times by mutual agreement. Pursuant to Section XV.D.8 of the Compact, modifications to the scope of gaming in the compact shall be amended automatically. The following amendments in this Memorandum of Incorporation (“MOI”) are hereby automatically incorporated in the Compact. Modifications that require formal amendment or renegotiation will be addressed separately. Anything not specifically authorized or amended by this MOI but provided for in the Tribe’s Compact, any other appendices, or the Most Favored Nations Section XV.D.8 shall remain in full force and effect.

**1. Compact, Section III.O is replaced in its entirety to read as follows:**

0. Prohibition on Firearms

The possession of firearms by any person within the Gaming Facilities shall be strictly prohibited, and the Gaming Operation shall post a notice of this prohibition near any entrance to the Gaming Facilities.

1. This prohibition shall not apply to:
  - (a) Local Law Enforcement or Tribal Law Enforcement agencies authorized by federal law, Tribal law or by a cooperative, mutual aid or cross-deputization agreement;
  - (b) Tribal or State Gaming Agencies;
  - (c) Individuals authorized by the Tribe’s ordinance to carry firearms in their employment capacity within the Gaming Facilities that:
    - (1) Obtain a State concealed weapons permit or similar license issued by the Tribe;
    - (2) Receive initial and ongoing firearms safety training; and
    - (3) Meet any other qualification requirements determined by the Tribe.
2. The Tribe will maintain a current list, including pictures, of persons authorized by the Tribe to carry firearms in the Gaming Facilities. The Tribal Gaming Agency will ensure the current list is available to the State Gaming Agency.

3. Tort liability for the negligent use of firearms by Tribal Law Enforcement, the Tribal Gaming Agency's employees, and employees of the Gaming Facilities while acting in an official capacity shall be addressed by the Tribe in its laws and regulations. Notice of these laws and regulations shall be prominently posted at each Gaming Facility in a public area. The State is exempted from liability regarding the permitted use of firearms by the Tribe authorized in the gaming facilities

**2. Add Appendix T Technical Requirements Governing the Gaming Data Environment.**

Appendix T "Technical Requirements Governing the Gaming Data Environment" is added to the Compact, in the form attached to this MOI, in its entirety.

**3. Add Appendix W governing Wide Area Progressives.**


- (1) Compact Section III.A, as previously amended, is amended to add:

31. Wide Area Progressives, subject to Appendix W.

- (2) **Appendix W "Rules Governing Wide Area Progressives"** is added to the Compact, in the form attached to this MOI, in its entirety.

**INCORPORATED ON THE LAST DATE ENTERED BELOW:**

KALISPEL TRIBE OF INDIANS

BY: 

GLEN NENEMA  
Chairman

DATED: 3-28-23

APPROVED


STATE OF WASHINGTON

BY: 

JAY INSLEE  
Governor

DATED: 4-17-23

UNITED STATES DEPARTMENT OF THE INTERIOR



Bryan Newland  
Assistant Secretary - Indian  
Affairs

6-8-2027  
Date

**KALISPEL TRIBE OF INDIANS and the  
STATE OF WASHINGTON  
CLASS III GAMING COMPACT**

**APPENDIX T  
Technical Requirements Governing the Gaming Data Environment**

**TABLE OF CONTENTS**

STATEMENT OF CONDITIONS AND LIMITATIONS.....	1
1. Definitions..... ;.....	1
2. Internal Controls.....	3
3. Change Management.....	3
4. Risk Assessment.....	4
5. Incident Response Plan.....	4
6. Disaster Recovery Plan.....	4
7. Network Hardware: Physical Access Controls and Security.....	4
8. Network Hardware: Physical Ports and Wired Connections.....	5
9. Network: Firewalls.....	6
10. Network: Password Protection and Logins.....	8
11. Network: Multi-layered Protection.....	9
12. Network: Encryption - Transmission and Storage.....	10
13. Network: External Connections.....	10
14. Network: Antivirus and Malware Protection Programs.....	10
15. Network: Software Updates and Patches.....	11
16. Network: Vulnerability Scanning and Penetration Testing.....	11
17. Network: Logging.....	12
18. Network: Clock Synchronization.....	13
19. Network: Remote Access.....	13
20. Wireless Networks.....	14

**CLASS III GAMING COMPACT**  
**APPENDIX T**  
**Technical Requirements Governing the Gaming Data Environment**

STATEMENT OF CONDITIONS AND LIMITATIONS

The Kalispel Tribe of Indians (Tribe) and the State of Washington (State) believe that conducting Class III gaming under the terms, limitations, and conditions set forth below will benefit the Tribe and the State, will be fair and protect the members of the Tribe and the other citizens of the State, and is consistent with the objectives of the federal Indian Gaming Regulatory Act. The parties have agreed upon conditions of the terms, provisions, and limitations contained in this Appendix T.

This Appendix describes the minimum network security requirements applicable to Gaming Data and the Gaming Data Environment related to the Tribal Lottery System as authorized in the Compact and necessary to prevent the unauthorized access, modification, destruction, or disclosure of Gaming Data. This Appendix addresses security areas in Appendix X2 Sections: 3.7.1, 5.11, 5.11.1, 5.11.2, 7, 7.1.9, 8.1.5, and replaces Appendix X2 Sections 9.1, 9.2, 9.3, 9.7, 9.7.1, 9.9, 9.10. Unless and until subsequently amended pursuant to the processes set forth in the Compact, this Appendix does not authorize any additional gaming activities, features, or connections not specifically authorized in this Appendix. Any provisions of the Compact and Appendices that are not addressed or replaced by this Appendix remain in full force and effect. This Appendix becomes effective as of the date the Gaming Operations IT Department demonstrates it can achieve compliance with all of its provisions as approved by TGA and SGA.

All terms not defined herein shall have the same definitions as in the Tribe's Compact and its amendments and appendices.

**1. Definitions**

Any capitalized term used but not defined herein shall have the same meaning as in the Compact.

**Approved Scanning Vendor (ASV)** is an independent technical expert selected by the Gaming Operation, licensed by the Tribal Gaming Agency, and certified by the State Gaming Agency to perform system integrity and security assessments of the Gaming Data Environment.

**Demilitarized Zone (DMZ)** is a perimeter network that protects an organization's internal local-area network (LAN) from untrusted traffic. A common Demilitarized Zone (DMZ) meaning is a subnetwork that sits between the public internet and private networks.

**Disaster Recovery Plan** means a written plan for processing critical applications and preventing loss of data in the event of a major hardware or software failure or destruction of facilities.

**Encryption** means Standard algorithms validated by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program.

**Gaming Data** means any information used in conjunction with a gaming system to determine outcome, payment, redemption, and the tracking of patron information.

**Gaming Data Environment** means the people, processes and technology(s) that store, process, or transmit Gaming Data.

**Incident** means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies

**Incident Response Plan** means the documentation of a predetermined set of instructions or procedures when a malicious cyber-attack is encountered against an organization's IT systems(s).

**Intermediate Distribution Frame (IDF)** means a cable rack that interconnects and manages the Gaming Data Environment network and wiring between a Server Room and network devices

**Intrusion Detection System - (IDS)** means Software that looks for suspicious activity and alerts administrators.

**Intrusion Prevention System - (IPS)** means network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

**Server Room** means the facility that centralizes a Gaming Operation's shared IT operations and equipment for the purposes of storing, processing, and disseminating data and applications.

**Sensitive Personal Identifiable Information- (PII)** means Social Security Numbers, driver's license numbers, Alien Registration numbers, financial records, biometrics, or a criminal history.

**System Components** means a discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system.

## **2. Internal Controls**

- 2.1 Detailed Internal Controls must identify the processes and procedures necessary to ensure the Gaming Data Environment network is configured and operated with the level of security described by this document. The Internal Controls must be developed, implemented, and maintained by the Gaming Operation consistent with Compact Section XI requirements and include at a minimum the following:
- a) A detailed description of the processes for approving and testing all network connections.
  - b) Define groups or individuals and their related roles and responsibilities within the organization for management and security of the Gaming Data Environment to provide for the segregation of incompatible functions.
  - c) Employee awareness training, which occurs at the time of hire and annually thereafter.
- 2.2 The Internal Controls will detail configuration standards for all System Components within the Gaming Data Environment. These Internal Controls will address vulnerabilities consistent with current, industry-accepted standards listed in the provisions of this Appendix.
- 2.3 The Internal Controls will require an inventory of System Components within the Gaming Data Environment be maintained by the Gaming Operation's Information Technology (IT) Department.

## **3. Change Management**

The Gaming Operation's IT Department must create a change management plan describing the processes and procedures for implementing and recording changes within the Gaming Data Environment that follow industry standards outlined in Gaming Laboratories International's GLI's Change Management Program (CMP) Guide, as now or hereafter amended. The initial plan, and any subsequent changes to the plan, must be approved by Tribal Gaming Agency.

#### **4. Risk Assessment**

The Gaming Operation must establish a risk assessment plan that outlines the process of identifying risks to organizational operations, specifically as it relates to technology. The initial plan, and any subsequent changes to the plan, must be approved by Tribal Gaming Agency. The plan must include at least the following:

- a) Is performed upon significant changes to the Gaming Data Environment;
- b) Identifies critical assets, threats, and vulnerabilities; and
- c) Results in a formal, documented analysis of risk.

#### **5. Incident Response Plan.**

A detailed Incident Response Plan must be developed, implemented, and maintained by the Gaming Operation's IT Department to ensure network security threats are responded to in a timely and effective manner should preventive measures fail or be compromised. The initial plan, and any subsequent changes to the plan, must be approved by Tribal Gaming Agency. The plan must include at least the following:

- a) Define roles and responsibilities during an Incident.
- b) Define a communication plan both internally and externally.

#### **6. Disaster Recovery Plan**

A detailed Disaster Recovery Plan must be developed, implemented, and maintained by the Gaming Operation's IT Department. The initial plan, and any subsequent changes to the plan, must be approved by Tribal Gaming Agency. The plan must include at least the following:

- a) Gaming Data backups must be maintained and sent off-site at regular intervals, as determined by the Gaming Operation's IT Department, and retained for a period of at least two years;
- b) Encryption must be applied for all off-site backups;
- c) A method of verifying the backup was successful.

#### **7. Network Hardware: Physical Access Controls and Security**

##### **7.1 Surveillance Requirements.**

All System Components, except wiring, cables, and conduit, in the Gaming Data Environment located in areas open to the public must have the ability to be effectively and clandestinely monitored and recorded by means of a closed circuit television system or digital surveillance system in accordance with Tribal-State Compact and/or Appendix A.



- 7.2 Server Rooms / Intermediate Distribution Frame (IDF) Access and Surveillance.
- a) Server Rooms / Intermediate Distribution Frame (IDF) must be secured using locked entry points and/or a swipe card system, or similar mechanism, capable of logging and/or controlling all entries to rooms in which systems hosting Gaming Data are present.
  - b) Server Rooms / Intermediate Distribution Frame (IDF) must have the ability to be effectively and clandestinely monitored and recorded by means of a closed-circuit television system or digital surveillance system in accordance with Tribal-State Compact and/or Appendix A.
  - c) A Server Room access record must include at least the following: the time, date, and purpose of entering, and the name and employee number (or other personal identification specific to such person) of the person doing so. Individuals providing product and warranty support that are not licensed by the Tribal Gaming Agency and certified, determined eligible, or registered by State Gaming may be allowed limited access when approved by the Tribal Gaming Agency, provided the individual is escorted at all times by an authorized Gaming Employee and the Gaming Employee must monitor their activity to ensure at no time during their work, the vendor accesses any server, program, console or shell that would display protected Gaming Data or perform any task outside the scope of work needed to complete the repair/upgrade.
  - d) Logs must be routinely reviewed by the Tribal Gaming Agency for any unauthorized access.
  - e) Server rack/cabinets must be securely locked and access restricted to authorized Gaming Employees.

7.3 Physically secure all media

All media containing Gaming Data shall be physically secured to prevent unauthorized access. Access controls and procedures for distribution must be described in the Internal Controls.

## **8. Network Hardware: Physical Ports and Wired Connections**

### 8.1 Networking Devices

- a) All networking devices located in areas accessible by the public, except for wiring, cables, and conduit must be in a locked, secure enclosure with key

controls in place. Access to networking devices must be restricted to authorized Gaming Employees only.

- b) Keys which provide access to any locked compartment, component or area of the Gaming Data Environment, as well as passwords, keycards, or PIN numbers used for access must be maintained and used in accordance with the access control standards enacted in the Tribe's statement of minimum Internal Controls.

#### 8.2 Unnecessary Services and Ports

Networking devices must have unnecessary and unused services turned off and non-essential ports disabled to prevent access.

- a) Additional security features must be implemented for any required services, protocols, or daemons that are considered to be insecure.
- b) All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers must be removed.

### 9. Network: Firewalls

Implementation of firewalls is required and the following must apply:

#### 9.1 Internal Controls

- a) The Internal Controls will describe the requirements for reviewing firewall and router rule sets.
- b) Current network diagrams that identify all connections between the Gaming Data Environment and other networks, including any wireless networks must be available to Tribal Gaming Agency and State Gaming Agency upon request.
- c) Current diagrams that show all Gaming Data flows across systems and networks must be available to Tribal Gaming Agency and State Gaming Agency upon request.

#### 9.2 Firewall and router configurations must restrict connections between untrusted networks and any System Components in the Gaming Data Environment.

- a) Firewalls must restrict in-bound and outbound traffic to that which is required for the Gaming Data Environment, and specifically deny all other traffic.
- b) Perimeter firewalls must be installed between all wireless networks and the Gaming Data Environment and must be configured to deny or permit only authorized traffic between the wireless environment and the Gaming Data Environment.

- 9.3 Firewalls must prohibit direct public access between the internet and any system component in the Gaming Data Environment and must:
- a) Implement a Demilitarized Zone (DMZ) to limit inbound traffic to only System Components that provide authorized publicly accessible services, protocols, and ports;
  - b) Limit inbound internet traffic to IP addresses within the DMZ;
  - c) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network;
  - d) Not allow unauthorized outbound traffic from the Gaming Data Environment to the internet;
  - e) Permit only authorized gaming activity connections into the network;
  - f) Place System Components for Gaming Data in an internal network zone, segregated from the DMZ and other untrusted networks;
  - g) Not disclose private IP addresses and routing information to unauthorized parties.
    - i. Remote management of firewall technologies must be via encrypted communications.
    - ii. Firewall policies must be reviewed, tested, and audited, at least annually and documented by the Gaming Operation's IT Department and audited by Tribal Gaming Agency.

9.4 Multiple Networks

In the event a particular network server is utilized in conjunction with other networks, all communications, including remote access, must pass through at least one approved application-level firewall and must not have a facility that allows for an alternate network path. If an alternate network path exists for redundancy purposes, it must also pass through at least one application-level firewall.

9.5 Firewall Audit Logs.

The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

- a) all changes to configuration of the firewall;
- b) all successful and unsuccessful connection attempts through the firewall;
- c) the source and destination IP addresses and port numbers for ingress traffic; and
- d) Media Access Control (MAC) addresses for egress traffic. At a minimum, the initial successful connection with a new MAC address.
- e) Audit logs must be maintained for a minimum of 2 years.

## **10. Network: Password Protection and Logins**

### 10.1 Unique Identification and Password Requirements for Users

- a) The Gaming Operation's Network Management Plan, as approved by the Tribal Gaming Agency, will require assigning unique identification to each user and administrator and ensure proper user-authentication management for users and administrators on all System Components by employing at least one of the following methods to authenticate all users:
  - i. Something you know, such as a password or passphrase;
  - ii. Something you have, such as a token device or card;
  - iii. Something you are, such as a biometric.

### 10.2 Device Passwords and Settings

- a) Device passwords must be immediately changed before, or upon, device installation and must conform to requirements set forth by the Gaming Operation's Network Management Plan as approved the Tribal Gaming Agency. All vendor-supplied default accounts and all unnecessary default accounts must be removed or disabled before implementation. This applies to all default passwords, including but not limited to those used by operating systems, software that provides security services, applications and system accounts.
- b) Networking devices must be configured to retain their current configuration, security settings, passwords, etc., during a reset or reboot process; For wireless environments connected to the Gaming Data Environment or transmitting Gaming Data, all wireless vendor defaults must be changed upon installation, including but not limited to default wireless Encryption keys, passwords, and Simple Network Management Protocol (SNMP) community strings.
- c) All passwords must be changed on a schedule established in the Network Management Plan.
- d) Shared accounts are prohibited.
- e) Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active.
- f) Access for employees who have been terminated, suspended or transferred to other departments must be removed in cases where that employee's new job function are no longer related to their previous access rights must be removed in accordance with the Tribe's Internal Controls;

- g) Remove/disable inactive user accounts after inactivity on a schedule established in the Network Management Plan.
- h) Thresholds must be configurable to allow a finite number of unsuccessful logon attempts via a given user's password in accordance with the Tribe's Internal Controls. Once the threshold is exceeded, the account must require administrative intervention to unlock.

### 10.3 Application Logins

All network users must have a unique identifier (user ID or login) for their specific use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

- a) User IDs must be capable of tracing activities to the responsible individual. Regular user activities must not be performed from Administrator Accounts.
- b) All access to any database containing Gaming Data is restricted as follows:
  - i. All user access to, user queries of, and user actions on databases are through programmatic methods. Tribal Lottery Game Set data, unredeemed Tribal Lottery System voucher data, and Sensitive PII may not be accessed or queried by applications or users originating outside of the Gaming Data Environment. External Access to Gaming Data may be authorized provided the proposal maintains the security and integrity of the information, is agreed to by the Tribe and the State Gaming Agency, and documented in a Memorandum of Understanding.
  - ii. Only database administrators, data analyst, and those with approved and defined role responsibilities have the ability to directly access or query databases
  - iii. Application IDs for database applications can only be used by the applications and not by individuals, users or other non-application processes.

## 11. Network: Multi-layered Protection

Multi-layered protection must be deployed to keep any successful intrusions isolated. Networks with different functions must be implemented separately. Multiple security layers must be implemented to complement one another insofar as what one misses, the other catches.

## **12. Network: Encryption - Transmission and Storage**

### **12.1 Transmission Encryption Technologies**

All networks and security protocols must deploy and support Encryption suited to the communication method for the transmission of confidential or sensitive data/information. At a minimum, highly personal information such as PINs and Social Security Numbers, vouchering information, game sets, Personally Identifiable Information would be confidential. The importance of other data may vary as a function of how critical that data is to the integrity of the network and/or the needs of the business.

### **12.2 Stored Gaming Data Encryption**

- a) Anywhere Gaming Data is stored must utilize strong Encryption.
- b) Databases used to store Gaming Data must be configured to enable Encryption by default. The Encryption of sensitive database fields is also acceptable if another method is used to prevent network sniffing.

## **13. Network: External Connections**

External connections to operational networks must be routed through secure gateways with Encryption.

- a) Where data sensitivity dictates, strong authentication, such as challenge/response devices, one-time passwords, tokens, Kerberos, smart cards, or similar protocol must be used once permission to connect has been granted.
- b) External connections must be removed or disabled when no longer required to prevent inadvertent reconnection.

## **14. Network: Antivirus and Malware Protection Programs**

Antivirus and malware programs must be utilized for network security purposes and must:

- a) Be mandatory and kept current on all Gaming Data Environment systems.
- b) Be updated automatically, or if not feasible or possible due to other constraints, be updated regularly through some manual means. If manual updates are required, their frequency must be stated in the IT Department's Internal Controls.
- c) Include both file system scanning and real-time processing.
- d) Ideally leverage multiple vendor, solutions between host systems and gateway services (e.g., email gateway).
- e) Generate audit logs which are retained for a minimum of 2 years.
- f) Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by Tribal Gaming Agency on a case-by-case basis for a limited time period.

- g) Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.

### **15. Network: Software Updates and Patches**

The Internal Controls must outline roles and responsibilities for software updates and patch management that cover the following activities:

- a) The Gaming Operation IT Department must proactively monitor and address software vulnerabilities of all network devices, including but not limited to routers, firewalls, switches, servers, and storage devices, by ensuring that applicable patches are acquired, tested, and installed consistent with IT Department's change management plan.
- b) Where possible, patches must be installed and validated in a test environment prior to their introduction to a production environment. Testing will help to expose detrimental impacts to software applications and/or network devices prior to implementation in a live network.
- c) Where possible, the installation of patches must be completed with the use of automated tools and the status of deployed patches must be monitored.
- d) Where possible, systems configurations must be backed up prior to patch installation.

### **16. Network: Vulnerability Scanning and Penetration Testing**

- 16.1 Network and host vulnerability scanners and penetration tests must be used to test for the vulnerabilities of internal network devices, applications, and network perimeter defenses, as well as adherence to security plan and standards. A process must be established to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.
- 16.2 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved. Scans must be performed by qualified Gaming Employees.
- 16.3 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV). Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved.
- 16.4 Vulnerability scanners must have the ability to handle the following minimum tasks:
  - a) Inventory systems and services including applied patches.
  - b) Identify security holes by confirming vulnerabilities.

- c) Provide comprehensive reports and charts for effective decision-making and improved security.
  - d) Define and enforce valid security policies when used during security device installation and certification.
- 16.5 Internal and external penetration testing must be conducted at least annually by an Approved Scanning Vendor.
- 16.6 The ASV must complete a report of all vulnerabilities found during penetration testing. A copy of the report will be provided to the Gaming Operation's IT Department and to the Tribal Gaming Agency and State Gaming Agency upon completion.
- 16.7 All exploitable vulnerabilities must be corrected by the IT Department and documented in a report provided to the Tribal Gaming Agency and State Gaming Agency and testing be repeated after corrections are made to verify the vulnerability has been addressed.

## **17. Network: Logging**

- 17.1 Security Logging.
- a) Automated audit trails for all Gaming Data Environment components must record the following events:
    - i. All individual user accesses to Gaming Data
    - ii. All actions taken by any individual with root or administrative privileges
    - iii. Access to all audit trails
    - iv. Failed login attempts
    - v. Use of and changes to identification and authentication mechanisms
    - vi. Initialization, stopping, or pausing of the audit logs
    - vii. Creation and deletion of any component that is required for operation, including but not limited to database tables, stored procedures, application executables and configuration files, system configuration files, static and shared libraries and Dynamic Link Library (DLL), system executables, device drivers and device configuration files, and third-party components.
  - b) Automated Audit trails must record at least the following entries for all Gaming Data Environment components for each event as follows:
    - i. User identification
    - ii. Type of event



- iii. Date & Time
- iv. Success, or failure indication
- v. Origination of event
- vi. Identify or name of affected data, system component, or resource

- 17.2 Automated Audit trails must be secured so they cannot be altered by:
- a) Limiting viewing of audit trails to those with a job-related need.
  - b) Protecting audit trail files from unauthorized modifications.
  - c) Backing up audit trail files to a centralized log server.
  - d) Writing logs for external-facing technologies onto a secure, centralized log server or media device.
  - e) Use file-integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts.

- 17.3 Gaming Operation's IT Department personnel, other than the system administrator, must review logs and security events for all System Components to identify anomalies or suspicious activity.
- a) Review all security events at least daily
  - b) Follow up on exceptions and anomalies identified during the review process.
  - c) Retain audit trail history for at least two years, with a minimum of three months immediately available for analysis.
  - d) Suspicious activities will be reported to Tribal Gaming Agency.

### **18. Network: Clock Synchronization**

To facilitate logging, the clocks of all relevant information processing systems within an organization or security domain must be synchronized with an agreed upon and accurate time source.

- a) Using time-synchronization, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.
- b) Critical systems have the correct and consistent time.
- c) Time data is protected.
- d) Time settings are received from industry-accepted time sources.

### **19. Network: Remote Access**

- 19.1 Remote access is any access to the Gaming Data Environment outside of the 'trusted' network. Remote access, where permitted, must authenticate all computer systems based on the authorized settings of the network or firewall application that establishes a connection with the network. The security of remote access will be

reviewed in conjunction with the current technology and approval from Tribal Gaming Agency and State Gaming Agency.

- 19.2 Remote Access Requirements. All remote access to the Gaming Data Environment must use multi-factor authentication and meet the following requirements:
- a) A remote access user activity log must be maintained as described below;
  - b) No unauthorized remote user administration functionality, such as adding users, changing user permissions or similar actions, must be permitted;
  - c) No unauthorized access to a database is allowed;
  - d) Authorized access to a database for information retrieval using existing functions is allowed;
  - e) A network filter (firewall) must be installed to protect access.
  - f) Enabled only during the time period needed and disabled when not in use. Monitored when in use.
  - g) Limit repeated access attempts by locking out the user ID after a finite number of unsuccessful logon attempts in accordance with the Tribe's Internal Controls.
  - h) Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
  - i) If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
- 19.3 Remote Access Log Auditing. The network server must create and maintain an activity log either automatically or have the ability to manually enter the logs depicting all remote access information. Remote access logs must minimally include the following:
- a) Log-on name and Tribal Gaming Agency license number of the user;
  - b) Time and date the connection was made;
  - c) Duration of connection; and
  - d) Activity while logged in, including the specific areas accessed and changes that were made.

## **20. Wireless Networks**

The wireless interface defines the communication boundary between two entities, such as a piece of software, a hardware device, or the end-user. It may also provide a means of translation between entities, which do not speak the same language. This section deals with software interfaces which exist between separate hardware and software components that

compose the wireless system, and which provide a programmatic mechanism such that these components can communicate.

- 20.1 **Communication Protocol.** Each component of a wireless network must function as indicated by the communication protocol implemented. All communication between the server(s) and an approved mobile device must use appropriate authentication and cryptographic protocols to provide mutual authentication of the mobile device and the server, ensuring the integrity of the data communicated, and for confidentiality, encrypting the data communicated. Commercially available IEEE 802.1x or higher industry authentication standard protocol-compliant devices are required when used in conjunction with other applicable security conscience components. The use of pre-shared keys is prohibited.
- 20.2 **Wireless Server Used with Other Systems.** In the event the wireless server is utilized in conjunction with other systems, including remote access, all communications must pass through at least one application-level firewall, and must not have capabilities that allow for an alternate network path unless the alternate route conforms to the requirements of this document, and has independent security (i.e. the keys are not the same as other networks).
- 20.3 **Wireless Network Physical Security.** All wireless networks must conform to the following minimum requirements:
  - a) Wireless access points must be physically located or secured such to prevent unauthorized access;
  - b) The wireless network must be an independent and isolated network in accordance with multiple layering techniques.
  - c) The network must support monitoring for evidence of unauthorized entry. If entry has been detected, the network must assert appropriate controls to lock down or disable the suspected entry point, if possible, and notify the Gaming Operation's IT Department; and
  - d) The network must retain evidence of any physical tampering of hardware components.
- 20.4 **Wireless Network Software Security.** A wireless network must:
  - a) Employ Encryption and strong user authentication, with a recommendation of at least two methods of validation prior to opening a wireless session;

Acceptable methods include: Username and password, a physical token, smart ID card, etc.;

- b) Perform mutual authentication to ensure that clients only communicate with valid networks.
- c) Maintain a list and/or database of authorized clients/devices, which it can communicate with. This list must include the client/device name, a unique client/device ID and the corresponding hardware identifier MAC
- d) Obfuscate the Service Set Identifier (SSID) so that what networks it is connected to are not immediately apparent.
- e) Close the active session if a user has exceeded the number of failed authenticated login attempts; the number of failed attempts must be configurable by the Gaming Operation's IT Department.
- f) Provide a printable report of failed network access attempts, including the time and date stamp, the device name, and the hardware identifier of all devices requesting access to the network; and make available to the Tribal Gaming Agency and State Gaming Agency upon request.

20.5 The use of strong user authentication, authorization, and Encryption, which will validate the user against a secure database is required. Communications between the network and the client device must use protocols designed for securing, authenticating, and encrypting wireless networks. One example of the appropriate protocol is IEEE 802.1x. It provides the framework required and permits the use of higher-level authentication methods in compliance with current industry standards.

20.6 Wireless Protocols and Communications. The IEEE 802.1x or higher industry authentication standard must be used with wireless networks and The Gaming Operation's IT Department must implement processes to test for the presence of rogue access points on at least a quarterly basis. A copy of the report will be provided to the Gaming Operation's IT Department and to the Tribal Gaming Agency upon completion.

**KALISPEL TRIBE OF INDIANS  
and the  
STATE OF WASHINGTON  
CLASS III GAMING COMPACT**

**APPENDIX W  
Rules Governing Wide Area Progressives**

**Table of Contents**

STATEMENT OF CONDITIONS AND LIMITATIONS.....	1
1. INTRODUCTION.....	1
1.1 Definitions.....	1
1.2 Intent.....	2
2. REQUIREMENTS.....	2
2.1 General Requirements.....	2
2.2 Submission Process.....	3
3. TESTING AND APPROVAL.....	4
3.1 Independent Gaming Test Laboratory.....;	4
3.2 General Testing Requirements.....	5
3.3 Materials Provided to Gaming Test Laboratory.....	5
3.4 Approval by the State Gaming Agency.....	5
3.5 Installation.....	6
3.6 WAP Operator Certification.....	6
3.7 Payment of Fees.....	6
4. INSPECTIONS.....	6
5. PARTICIPATION IN ANOTHER APPROVED WAP.....	7
5.1 Requirements for participation in another approved WAP:.....	7

**CLASS III GAMING COMPACT**  
**APPENDIX W**  
**Rules Governing Wide Area Progressives**

STATEMENT OF CONDITIONS AND LIMITATIONS

The Kalispel Tribe of Indians (Tribe) and the State of Washington (State) believe that conducting Class III gaming under the terms, limitations, and conditions set forth below will benefit the Tribe and the State, will be fair and protect the members of the Tribe and the other citizens of the State, and is consistent with the objectives of the federal Indian Gaming Regulatory Act. The parties have agreed upon conditions of the terms, provisions, and limitations contained in this Appendix W.

This Appendix contains interdependent conditions and consequences that must be accepted as a whole in order to operate or participate in a Wide Area Progressive (WAP). As a result, authorization to operate or participate in a WAP requires the Tribe to operate and participate in accordance with all of the requirements of both this Appendix and the subsequent memorandum of understanding agreed to under subsection 2.2.3.

1. INTRODUCTION

1.1 Definitions

Any capitalized term used but not defined herein shall have the same meaning as in the Compact.

“Component” means hardware, software, and any integral parts or combination thereof necessary to operate the WAP.

“Fair” means the odds of winning prizes being equal to other devices connected to the same WAP within accepted statistical industry standards as verified by an approved Gaming Test Laboratory.

“Participant Tribe” means a tribal government within the State that has been accepted to join in a specific approved WAP.

“Progressive Prize” means a prize that increases by a predetermined amount based on play on a Class III Tribal Lottery System (TLS).

“Wide Area Progressive” or “WAP” means a jackpot sharing system between multiple participating jurisdictions and/or governments within and outside the State.

"WAP Controller" means a component at each participating jurisdiction's and/or government's gaming facility that accumulates Progressive Prizes and provides Progressive Prize information to display for players.

"WAP Operator" means the licensed manufacturer or gaming service supplier that maintains the WAP central system which communicates with individual WAP Controllers.

1.2 Intent

The intent of the parties is to allow the Tribe to use a WAP where players are entered into a pool for a Progressive Prize without the insertion of additional consideration.

1.2.1 The WAP must be Fair, secure, and auditable.

1.2.2 The WAP does not constitute a mechanical gambling or lottery device activated by the insertion of a coin or by the insertion of any object purchased by any person taking a chance by gambling in respect to the device.

1.2.3 The WAP does not constitute an electronic or mechanical device or video terminal which allows for individual play against such device or terminal.

2. REQUIREMENTS

2.1 General Requirements

The basic requirements for a WAP authorized under Section III.A-Scope of Class III Gaming Activities of the Compact are as follows:

2.1.1 Any WAP Controller utilized by the Tribe may operate only in conjunction with the TLS and may not offer a game where the player may play against the device.

2.1.2 The restrictions on the use and operation of the TLS as governed by Appendix X and Appendix X2, including prohibiting individual play against such devices or terminals, are not changed by this Appendix.

2.1.3 The WAP will be Fair for players in the State.

2.1.4 The rules of play will be posted for the customer.

2.1.5 The WAP will conform with 25 U.S.C. § 2710 (d)(1)(A), (B), and (C).

2.1.6 The WAP will allow the State Gaming Agency to remotely view the Tribe's reports and activity in real time as specifically provided for in a full submission.

2.1.7 The Tribe will make available for review agreements and contracts regarding WAP participation in accordance with Compact Section VII.B Access to Records.

- 2.1.8 Employees and/or representatives of a WAP Operator must meet the applicable licensing and certification requirements in accordance with Compact Section IV Licensing and Certification Requirements and V Licensing and Certification Procedures.
- 2.1.9 Each specific type of WAP approved will conform to the standards documented in a Memorandum of Understanding after a full submission has been approved, and the Tribe shall not begin operation of said WAP until the testing and certification requirements referred to in Section 3 of this Appendix are met.
- 2.1.10 The Tribe will notify the State Gaming Agency of its participation in a specific type of WAP and will follow the requirements in an approved Memorandum of Understanding for the specific type of WAP in order to participate in that WAP.

2.2 Submission Process

- 2.2.1 Each full submission made must meet the requirements contained in the Compact, Appendix X, Appendix X2, and this Appendix, and shall set the technical standards and Internal Controls for the operation of that type of WAP. Except for the TLS as governed by Appendix X or X2, the Tribe and the State Gaming Agency shall enter into a separate Memorandum of Understanding for each specific type of WAP the Tribe wishes to operate.
- 2.2.2 A "full submission," as that term is used in this Appendix, shall include a detailed description of technical standards and other information that includes at least the following:
  - 2.2.2.1. How the system operates with the TLS, including connections to the system and other jurisdictions, probability, and summary of game rules which must be posted for the customer in any format;
  - 2.2.2.2. WAP illustrations, schematics, block diagrams, circuit analyses, program object and source codes, and hexadecimal dumps which means the compiled computer program represented in base 16 format;
  - 2.2.2.3. Technical and operation manuals including operation, interface, Progressive Prize verification, and random number generator standards;
  - 2.2.2.4. System hardware specifications including all key Components including the WAP Controller;
  - 2.2.2.5. Base software which means the software platform upon which games are loaded;
  - 2.2.2.6. Game software for one or more games, including game set size and point of overlap;
  - 2.2.2.7. System security including encryption, firewalls, key controls, and surveillance;
  - 2.2.2.8. Odds for winning the Progressive Prize, the base Progressive Prize amount, the reset Progressive Prize amount, the incremental increases of the Progressive Prize, and any secondary pool increment(s);
  - 2.2.2.9. Accounting system requirements and reports which must include at



- least a progressive balancing report and report of unusual events such as critical memory clears, changes to Progressive Prizes, offline equipment, multiple site prizes, and related reports;
- 2.2.2.10. Reports which must include at least a progressive summary, aggregate, and payoff and any adjustments made by the WAP Operator on Progressive Prize pools;
  - 2.2.2.11. Procedures for handling simultaneous Progressive Prize winners in multiple locations or jurisdictions;
  - 2.2.2.12. Procedures to make changes or adjustments to or be removed from the WAP, including notice requirements to the Participant Tribes and players;
  - 2.2.2.13. Procedures for accepting additional Participant Tribes or participating jurisdictions and/or governments into the WAP;
  - 2.2.2.14. Procedures to handle system malfunctions and reporting those malfunctions to participating jurisdictions and/or governments;
  - 2.2.2.15. Player dispute procedures;
  - 2.2.2.16. Procedures, including a timeframe, for Gaming Operations staff or WAP Operator to provide notice to the Tribal Gaming Agency and State Gaming Agency of WAP non-compliance;
  - 2.2.2.17. Capability and process to allow the State Gaming Agency to remotely view the Tribe's WAP to review reports and activity real time; and
  - 2.2.2.18. Any agreement, written specifications, or limitations required of a WAP Operator by any other state or tribal government and affecting a WAP.
- 2.2.3 The Tribe may present to the State Gaming Agency, at any time, a WAP full submission it believes satisfies the requirements of the Compact and this Appendix. Within ninety (90) days of the Tribe's providing of a complete, full submission for its proposed WAP to the State Gaming Agency, the Tribe and the State Gaming Agency will execute a Memorandum of Understanding as required by Section 2.1.9.

### 3. TESTING AND APPROVAL

#### 3.1 Independent Gaming Test Laboratory

- 3.1.1 Designation. The Tribe shall select one or more gaming test laboratories (hereinafter "Gaming Test Laboratory") to perform the testing required in this Appendix. The selection of a Gaming Test Laboratory will be done according to Appendix X2, Section 10.1.
- 3.1.2 Gaming Test Laboratory Duty of Loyalty. The Tribe shall inform the Gaming Test Laboratory, in writing, that irrespective of the source of payment of its fees, the Gaming Test Laboratory's duty of loyalty and reporting requirements run equally to the State Gaming Agency and the Tribe.

3.2 General Testing Requirements

The general purpose of testing the WAP and related Components is to determine the compliance of the WAP with the Memorandum of Understanding agreed to by the Tribe and the State Gaming Agency. Prior to operation of the WAP, the WAP and related Components shall be tested by a licensed Gaming Test Laboratory, to verify:

3.2.1 Compliance with the applicable requirements of the Compact, Appendix X, Appendix X2, and this Appendix; and

3.2.2 The WAP is Fair for both the players and the participating gaming facilities; and

3.2.3 Compliance with the Memorandum of Understanding and currently accepted gaming test industry standards with respect to multi-jurisdictional WAPs.

3.3 Materials Provided to Gaming Test Laboratory

3.3.1 The Tribe shall provide or require that the WAP Operator provide to the Gaming Test Laboratory a copy of the executed Memorandum of Understanding, and any other information requested by the Gaming Test Laboratory. The Tribe shall make all such materials available to the State Gaming Agency upon request;

3.3.2 If requested by the Gaming Test Laboratory, the Tribe shall require the WAP Operator to transport not more than two (2) working models of the WAP associated player terminals, and any required system elements to a location designated by the Gaming Test Laboratory for testing, examination or analysis. Neither the State nor the Gaming Test Laboratory shall be liable for any costs associated with the transportation, testing, examination, or analysis, including any damage to the Components of the WAP. If requested by the Gaming Test Laboratory, the Tribe shall require the WAP Operator to provide specialized equipment or the services of an independent technical expert to assist with the testing, examination and analysis. The Gaming Test Laboratory will notify the State Gaming Agency of the request and need for the request;

3.4 Approval by the State Gaming Agency

Upon receiving the certification, technical standards tested, and results of testing from the Gaming Test Laboratory, the State Gaming Agency shall either approve or disapprove the WAP or Component thereof, based on the criteria contained in this Appendix and the Memorandum of Understanding. The Tribe or WAP Operator may request a temporary suspension of the State Gaming Agency's review of the WAP or Component for a mutually agreed upon time period through a written request to the State Gaming Agency Director.

During the State Gaming Agency approval process, the Gaming Test Laboratory will meet with the State Gaming Agency and respective Tribal Gaming Agency to inform regulatory staff of the certification process and technical standards tested and provide training so that these personnel have an understanding of the WAP, can create a regulatory program, and can better respond to questions and complaints.

3.5 Installation

3.5.1 No WAP may be offered for play unless:

3.5.1.1 Such WAP is approved as provided in this Appendix; and

3.5.1.2 The WAP prototype thereof has been tested and certified by the Gaming Test Laboratory as meeting the requirements and Memorandum of Understanding specified by this Appendix.

3.5.2 The State Gaming Agency and Tribal Gaming Agency will meet to confer on WAP initial implementation and Internal Controls changes to prepare for WAP operation. Initial Internal Controls and any subsequent changes are to be completed in conformance with Compact Section XI.A Adoption of Regulations for Operation and Management.

3.6 WAP Operator Certification

Before any Component of a WAP may be placed into operation, the Tribe shall first have obtained a written certification from the WAP Operator that, upon installation, each such Component:

3.6.1 Conforms to the specifications of the WAP as certified by the Gaming Test Laboratory; and

3.6.2 Operates and plays in accordance with the applicable requirements of the Compact, Appendix X, Appendix X2, this Appendix, and the Memorandum of Understanding.

3.7 Payment of Fees

3.7.1 The Gaming Test Laboratory shall not accept a WAP submission from a WAP Operator without first receiving an executed Memorandum of Understanding from the Tribe. All Gaming Test Laboratory fees related to a WAP submission shall be the responsibility of the WAP Operator.

3.7.2 All State Gaming Agency testing fees related to a WAP submission shall be the responsibility of the WAP Operator.

4. INSPECTIONS

4.1 The Tribe shall allow the State Gaming Agency to inspect any Components of a WAP for the purposes of confirming that such Component is operating in accordance with the requirements of the Compact, Appendix X, Appendix X2, this Appendix, and the Memorandum of Understanding and that such Component is identical to that tested by a Gaming Test Laboratory. Inspections shall be pursuant to the Compact.

4.2 The WAP Operator shall allow the Tribal Gaming Agency and State Gaming Agency to inspect any Components of a WAP for the purposes of confirming that such Component is operating in accordance with the requirements of the Compact, Appendix X, Appendix

X2, this Appendix, and the Memorandum of Understanding and that such Component is identical to that tested by a Gaming Test Laboratory.

- 4.3 When the Tribal Gaming Agency or State Gaming Agency determine there is a failure to comply with the Memorandum of Understanding, either will immediately suspend a WAP's operation.
- 4.4 Reinstatement of a WAP's operation shall occur once the Tribal Gaming Agency and State Gaming Agency agree that a suspended WAP complies with the Memorandum of Understanding as determined by follow-up testing by the Gaming Test Laboratory.
- 4.5 If after an investigation the Tribal Gaming Agency or State Gaming Agency believe the WAP is not operating in a Fair manner, either may request a mathematical review by an independent third party. The WAP Operator will pay the cost of this review.

## 5. PARTICIPATION IN ANOTHER APPROVED WAP

The Tribe may participate in more than one approved WAP. When the Tribe elects to participate in a WAP that has already been approved by the State Gaming Agency, Sections 1-4 of this Appendix do not apply except as required by Section 5.1.3 below.

### 5.1 Requirements for participation in another approved WAP:

- 5.1.1. When participating in a WAP that has already been approved by the State Gaming Agency, the Tribe must follow the requirements in the Memorandum of Understanding related to that WAP.
- 5.1.2. The Tribe will notify the State Gaming Agency of its participation in or withdrawal from another WAP and will make any and all copies of its participation agreements available for review.
- 5.1.3. When the Tribe participates in an already approved WAP, the Tribe will follow the requirements listed in Sections 1, 2.1, 3.5, 3.6, 4, and 5 of this Appendix.