

MEMORANDUM OF UNDERSTANDING BETWEEN
THE SQUAXIN ISLAND TRIBE
And
THE WASHINGTON STATE GAMBLING COMMISSION
REGARDING
REMOTE ACCESS TO THE (MANUFACTURER) TRIBAL LOTTERY SYSTEM
NON-FIXED PORTAL LOCATION

The Squaxin Island Tribe (Tribe) and the State of Washington (State) have executed a Class III Gaming Compact (Compact) in October of 1993 pursuant to the Indian Gaming Regulatory Act (IGRA) of 1988.

The Class III Gaming Compact executed by the Tribe and State, as well any amendments thereto, were approved by the Secretary of the Interior and are in full force and effect (hereinafter referred to as the “Compact”). The Tribe and State conducted additional negotiations in accordance with the provisions of IGRA and amended Section IV of the Compact by adding Appendix X to the Compact that authorized the Tribal Lottery Systems described therein.

Since the adoption of Appendix X, the Tribe and State have agreed to certain changes to the Tribal Lottery System known as Appendix X2. Section 5.11.1 of Appendix X2 allows for proposed modifications to allow components to be located outside of the Tribe’s gaming facilities, including the proposed rules, manner of regulation, and manner of play, monitoring and/or maintenance of the system.

Any proposal for modification as outlined in Section 5.11.1, requires submission to, and approval by, the Tribal Gaming Agency, the Squaxin Island Gaming Commission (TGA) and the State Gaming Agency, the Washington State Gambling Commission (SGA). Standards for the Tribal Lottery System’s components located outside of the Tribe’s gaming facilities (known as “remote access technical standards”) have been developed in cooperation with, and agreed upon by the Tribe and State.

Pursuant to Appendix X2 as set forth in the Third amendment to the Compact, both parties agree to the Tribal Lottery System’s Remote Access Technical Standards proposal provided by EVERI, which include requirements that EVERI adhere to, as follows:

- 1) **Technical Support**: As an element of technical support, an employee of Everi may perform an analysis of, or render technical support with regard to Everi’s approved Appendix X2 compliant Tribal Lottery Systems (TLS) from Everi’s portal site or approved remote access connection structure. Any remote access to this system shall be performed in accordance with the following procedures:

- a) Limited Access: Only an employee of Everi who is licensed by the TGA and certified or licensed by the SGA as a Class III gaming employee may remotely access a TLS sold, leased, or otherwise distributed by Everi for use at a licensed gaming facility; and
- b) Prohibited Actions: Employees of Everi shall be prohibited from remotely installing, manipulating, or deleting any Game Set or Game Subset software or data. The installation or modification of any other SGA approved TLS software is prohibited without prior notice to and approval by TGA and SGA; and
- c) System Access: Everi shall create system access that:
 - i) Requires the identification of each Everi employee that may be required to perform technical support from a remote location to follow the unique TLS system account established for the licensed gaming facility; and
 - ii) Prohibits unauthorized access to the operating system, any database, or any component of a TLS from a remote location or from Everi's portal site; and
 - iii) Requires prior notice be given to the TGA of the Everi's intent to remotely access a designated TLS; and
 - iv) Requires the TGA to take affirmative steps, on a per access basis, to activate Everi's access privileges; and
 - v) Requires approval by TGA and SGA prior to any remote installation or modification to network requirements, as referenced in Section 5.11 in Appendix X2, to protect the integrity of the TLS; and
- d) Log Maintenance: A log shall be maintained by both Everi and the TGA. Each log shall be retained by both Everi and TGA respectively for documentation and audit purposes as required in Appendix X2 Section 7.1.9. Each of the two logs must contain, at a minimum, the following information:
 - i) The specific components of the TLS accessed, including manufacturer; and
 - ii) The name and license number of the employee remotely accessing the TLS; and
 - iii) The name and license number of the TGA employee activating Everi's access to the TLS; and
 - iv) The date, time and duration of the connection; and
 - v) The reason for the remote access including a description of the symptoms or malfunction prompting the need for remote access to the TLS; and

- vi) Any action taken or further action required; and
- e) Remote Access Communications: In general, regardless of location, remote access communications between Everi and their TLS, as identified in this MOU, shall occur using a dedicated and secure communication protocol or application utilizing encryption in accordance with Appendix X2 Section 9.3 and the following standards:
 - i) Everi shall document and describe in detail the remote communication technology, application or protocols to be used for remote access into each gaming facility; and
 - ii) The communication protocol or application must ensure that remote access connections can only be made through the authorized Everi network access control structure. The system must refuse access to connection attempts made from outside of this structure; and
 - iii) Network connections used in remote access communications may utilize wireless networking technology, which must meet the following requirements:
 - a. Connections to wireless networks used to connect to the Everi network must use strong encryption. For example, use of encrypted wireless channels using Wi-Fi Protected Access 2 with Advanced Encryption Standard (WPA2-AES) or better encryption; and
 - b. Use of wireless technology for remote access may only be made from private locations where unauthorized individuals cannot view or access any information about the remote access session; and
- iv) Remote Access Procedures:
 - a. In general, regardless of location, Everi shall develop and enforce procedures which address assignment, complexity, maintenance, confidentiality, and recovery of employee usernames and passwords used for remote access. At a minimum, login credentials must:
 - i. Be unique to each individual user; and
 - ii. Be entered at each connection layer; and
 - iii. Use passwords that are complex enough to prevent easy guessing or cracking; and
 - iv. Not be shared with others; and
 - b. Virtual Private Network (VPN) technology with a minimum of 128 bit encryption must be used for remote access connections initiated from outside Everi's portal site. At a minimum:

- i. VPN access may only be through the use of Everi approved and issued computer hardware and access keys; and
 - ii. VPN access may only be granted through the use of at least a 2-factor authentication method such as appropriately issued RSA tokens; and
 - iii. Everi shall have security policies and procedures in place to ensure only authorized personnel are issued hardware and VPN access keys used for remote access; and
 - iv. For remote access connections originating outside Everi’s portal site, Everi shall ensure that all remote access connections are compliant with section 9.3 of Appendix X2.
- c. For remote access connections originating outside Everi’s portal site, Everi shall develop and enforce IT security standards to ensure casino information remains secure. Security standards must be at least equivalent to commonly accepted national and international best practices for IT security such as National Institute of Science and Technology (NIST) standards as they currently exist or may be amended in the future; and
- d. Laptops or computers used for remote access originating outside Everi’s portal site must meet the following requirements:
 - i. Employ full disk encryption; and
 - ii. Have a mechanism to detect and prevent installation of spyware, key loggers, hacking tools, or other malicious software; and
 - iii. Have regularly updated antivirus software; and
 - iv. Employ active firewall software; and
- e. For remote access connections initiated outside Everi’s portal site, Everi employees must be physically identified by TGA prior to connecting. Identification methods may include but are not limited to webcam photos, biometric technology, or voice telephone calls; and
- f. Everi employees making remote access connections initiated outside Everi’s portal site must not allow non-authorized individuals to observe session information. Everi must develop and enforce policies outlining these requirements; and
- v) Wide Area Network (WAN) Communications: The communications over the WAN must be secured from intrusion, interference, and eavesdropping via use of techniques such as VPN, encryption, authentication, etc. Furthermore, it must be disclosed what type of WAN communication is to be used as well as any proposed or actual changes to this connection type; and
- vi) Approved Access: Communication by Everi must be made through Everi’s portal site or approved remote access connection structure; and

- vii) Portal Site: Any remote access portal site shall be in a secured room, which is designed and constructed to provide maximum security for the remote access equipment contained therein. Security measures are to include effective and detailed video monitoring and recording of activities conducted within the remote access location. These recordings must be made available to TGA and SGA immediately upon request. Recorded activities shall be retained for a minimum of seven days, or longer as requested by TGA or SGA; and
- f) Remote Access Monitoring: Remote access monitoring capability shall be implemented by Everi, which performs, at a minimum, the following functions during each remote session:
 - i) Track and monitor all access to TLS components; and
 - ii) Track and retain remote access session information, including which unique user accessed the TLS; which files were accessed, modified, or transferred; any telnet activity; which hosts and services were accessed, as well as when, and for how long; and
 - iii) Record historical access or session information, including detailed log files in accordance to the standards of Appendix X2 Section 7.1.9; and
 - iv) End a remote session automatically or log off after a predetermined time of inactivity; and
 - v) Display and record video capture or desktop sharing session information in both real time and historically. The activities of each remote access session shall be available for viewing by TGA in real time. Recorded activities shall be retained by the communication protocol or application and made available to TGA for a minimum of seven days; and
 - vi) All remote access records shall be made available to the TGA or SGA immediately upon request; and
- 2) Provision of Working Model: Everi must submit and transport a working model of the remote access equipment and product to SGA. For the purpose of continued monitoring, the SGA may retain working models or components after approval for as long as the equipment is in use in the State; and
- 3) Approval Required of Remote Access Proposal: TGA and SGA shall either approve or disapprove a manufacturer's new or modified remote access proposal based on the technical criteria contained in this MOU; and

- 4) Notification of Loss of Access: Everi shall notify the SGA and TGA within 24 hours when an employee of Everi is no longer employed by, or authorized by, Everi to remotely access a TLS pursuant to this section; and
- 5) Alternative Provisions Permitted: The Tribe and SGA may agree on alternative provisions to those set forth herein, provided such provisions adequately preserve and protect the integrity and security of remote access into the TLS system; and
- 6) Compliance with Tribal-State Compact: The Tribal Gaming Operations' Policies and Procedures related to remote access will be processed as outlined in the Tribal-State Compact; and
- 7) Notification of Any Changes by Everi: Everi must immediately notify SGA and TGA of any changes to the remote access procedures, or entry procedures or which otherwise affect compliance with the MOU.

This Memorandum of Understanding shall remain in effect unless and until such time as either party notifies the other of intent to terminate the agreement or to request a change in the provisions set forth herein. Should either party wish to terminate this Memorandum of Understanding or change a provision herein, 60 days written notice shall be provided to the other party.

IN WITNESS WHEREOF, The Squaxin Island Tribe and the State of Washington have executed this Memorandum of Understanding.

Signed:

Kristopher Peters
Kristopher Peters (Jun 10, 2021 19:53 PDT)

Kris Peters, Chairman
 Squaxin Island Tribe

Date: Jun 10, 2021

 Tina Griffin, Interim Director
 Washington State Gambling Commission

Date: _____






MOU Remote Access-Non fixed portal location-Squaxin Island 2021

Final Audit Report

2021-06-11

Created:	2021-06-10
By:	Melissa Puhn (mpuhn@squaxin.us)
Status:	Signed
Transaction ID:	CBJCHBCAABAAymwl1GFQEhnH42U4cJlzUhOdJQOKLKEK

"MOU Remote Access-Non fixed portal location-Squaxin Island 2021" History

-  Document created by Melissa Puhn (mpuhn@squaxin.us)
2021-06-10 - 10:53:06 PM GMT- IP address: 216.235.106.129
-  Document emailed to Kristopher Peters (kpeters@squaxin.us) for signature
2021-06-10 - 10:53:26 PM GMT
-  Email viewed by Kristopher Peters (kpeters@squaxin.us)
2021-06-11 - 2:53:13 AM GMT- IP address: 174.204.71.175
-  Document e-signed by Kristopher Peters (kpeters@squaxin.us)
Signature Date: 2021-06-11 - 2:53:32 AM GMT - Time Source: server- IP address: 174.204.71.175
-  Agreement completed.
2021-06-11 - 2:53:32 AM GMT