2.4. The Parties shall immediately disable the access to Privacy Information of any worker (including its employees and authorized subcontractors) whose employment has been terminated.

2.5. The Parties shall adhere to NIST standards for the management of passwords to all systems containing Privacy Information.

3. Securing Infrastructure for Protecting Confidential Information

3.1. The Parties shall maintain appropriate barriers between untrusted networks (as defined above) such as the internet, and systems containing Privacy Information according to federal and state regulations through the use of accepted industry standards and practices.

(a) Adhering to a comprehensive procedure to review audit logs of all monitoring tools and to resolve any unauthorized access attempts, changes to either party's data and objects, and privileged or administrator-level access to either party's data files and objects.

(b) Disabling unnecessary programs and services that are installed by default with either party's overall software packages.

4. Physical Security of Facilities. The Parties shall maintain multiple layers of physical security separating unauthorized persons and systems from facilities that access, process, store, transmit or otherwise handle Privacy Information. The Parties shall maintain, in its data centers or third-party data centers (acting as agent), adequate environmental and power controls where hardware and equipment are located that is used to support business with or services for either party.

5. Training. The Parties will implement and maintain ongoing mandatory security training programs for all workers who have access to Privacy Information to emphasize the importance of data security in its organization. The Parties will periodically monitor its employees who have access to Privacy Information for compliance and will appropriately discipline employees for any data security violations.

6. Security Breach Notices. The Parties will maintain a formal incident response plan which shall include, at a minimum, the actions that shall be taken in response to a breach or suspected breach and the specific responsibilities of personnel to implement such actions. NSHE's plan shall address the obligations to provide notification of a breach under applicable state and federal breach notification laws. NSHE shall notify MGM of any breach or suspected breach involving Privacy Information. **Notice shall be provided by telephone (855) 286-0151 and email** mgm _soc@mgmresorts.com **with a copy in writing sent via reputable overnight courier to MGM Resorts International, Information Systems, 6770 Edmond, Las Vegas, NV, 89118 with a copy to MGM Resorts International, Corporate Legal, 6385 South Rainbow Boulevard, Las Vegas, NV 89118.** MGM shall notify NSHE of any breach or suspected breach involving Privacy Information. **Notice shall be provided by telephone (775) 789-3710 and email to** TDobbert@nshe.nevada.edu **with a copy in writing sent via reputable overnight courier to Thomas Dobbert, Chief Information Security Officer, Nevada System of Higher Education, 1664 N. Virginia St./Mail Stop 270, Reno, NV 89557-0023.** The Parties shall cooperate with each other, and/or its designee, to permit an investigation of the breach or suspected breach of