1.0 Responsibility

Physical security is the responsibility of every person at **Black Gaming, LLC** that Information Technology Infrastructure assets and data have been entrusted. The Data Centers Operation's are the responsibility of the Director of IT Support and the members of that team.

2.0 Purpose

The purpose of this policy is to restrict physical access to Information Technology Infrastructure assets at **Black Gaming, LLC** to only those with a business need to access it. The granting of physical access is the responsibility of the Director of IT Support and/or delegates. Restricting such access helps to prevent theft of computer equipment and any associated intellectual property it may contain.

This policy also addresses the daily operations of the **Black Gaming, LLC's** Data Centers.

3.0 Scope

This policy applies to all **Black Gaming, LLC's** Information Technology Infrastructure assets to include, but not limited to:

- Central Data Center and those located at each of the properties
- Monthly Maintenance Schedule for Information Technology Infrastructure
- Servers
- Network Infrastructure
- Desktops
- Laptops
- Backup Media
- Job Scheduling and Management

4.0 Policy

- All Information Technology Infrastructure Assets should be in a secured area with restricted access. Data Centers and telecommunications closets that can be locked must remain locked at all times. Access to Data Centers and telecommunications closets shall be the responsibility of the Director of IT Support and restricted to those that the Director grants formal authorized access to. Visitors shall be accompanied by authorized Information Technology employees and supervised at all times. Upon entry to a server room or telecommunications closet, the following shall be logged: visitors name, date and time of arrival, reason for entrance, date and time of departure, and IT Team member who escorted visitor. Exceptions must be authorized and approved by the Director of IT Support.
- The Director of IT Support is responsible for the Monthly Maintenance Schedule. All items scheduled for maintenance should have an approved Help Desk Ticket authorized by the Director prior to placement on the schedule, with the only exceptions being emergencies.
- Media used for Information Technology Infrastructure backups must be appropriately identified and stored in a locked and fireproof cabinet in the server room or a similar secured area. When backup media is removed from or transported between the Data Centers it must be transported in a secure container (e.g., lock box). Unused media containing sensitive information must be kept secure at all times.
- Retired Information Technology Infrastructure Assets and media, to include but not limited to backup tapes, hard drives, floppy disks, CDs, DVDs, and USB storage devices, must be securely

erased and/or physically destroyed before disposal. The IT department will secure all licensed software floppies and CDs in the server room or other secure area or in locked drawers or cabinets within the IT department.

- All hard copy documentation which supports the Information Technology Infrastructure should be stored in a secured area with restricted access.
- IT Team Members desktop and laptop screens should automatically lock after 15 minutes of inactivity and require the use of password to unlock the computer.
- The Director of IT Support is responsible for the Daily Job Schedule. Changes to the daily job schedule should be documented in a Help Desk Ticket and approved to be placed in to production by the Director. See Supplement 1 – Daily Job Schedule.
- Any breach of this policy should be logged in a Help Desk Ticket and followed with an investigation by the Director of IT Support. It is the responsibility of the Director of IT Support to manage the incident and take the appropriate action.

5.0 Enforcement

Management will determine appropriate use and enforce this policy. A violation of this policy will be acted upon immediately, and appropriate corrective action taken. Any violation of this Policy by the employee may result in disciplinary action, to and including, the following:

- Offenses will be reported to the employee's manager for review
- Probation
- Termination of employment
- Other disciplinary action
- Civil and/or criminal prosecution

6.0 Additional Information

Any inquiries relating to the Physical Security and Data Center Operations Policy should be directed to the Director of IT.