Physical Security Technical Document

The following are physical security best practices:

The casino must ensure that the computer room is secured at all times. Entry into the computer room must be limited to authorized individuals. Acceptable security measures could include but are not limited to:

- Cipher locks
- Door locks and keys
- Badge scanner
- Biometrics

A log entry must also be completed by an individual entering the computer room. The log must include, at a minimum, date, time in and time out, employee name, and reason for entry. The log must be reviewed by IT management or ICO if there is only one person on the IT staff. A review of the log must occur within the next calendar month. The reviewer must follow the requirements outlined in the Division's documentation standards.

The following is recommended for security:

- No doors that lead directly outside
- No Windows that lead directly outside
- Internal windows should be security/safety glass
- The room should be well lit
- Emergency lighting should be installed
- Portable lighting should be placed in close proximity to the entrance and tested every 6 months
- Incident response plan for unauthorized individuals in the computer room

Safeguarding against power fluctuations is critical in order to ensure availability of the data. The device or set of devices that are used to mitigate a power outage or electrical damage to the system must include a surge suppressor, and battery backup. The unit(s) should be connected to a dedicated circuit and have no other devices plugged into the socket.

The room should be maintained at the correct environmental specifications. All computer hardware manufacturers have a temperature range they state their equipment must be maintained in. Computer or infrastructure equipment should be free of dust and particles. Equipment that maintains temperature should have filters in the intake section of the system.

The computer room should be equipped with fire suppression. The suppression system or device should be rated for electrical fires.

All equipment should be installed to manufacturer's guidelines and should not exceed its stated lifecycle. For example if the batteries in the battery backup unit are rated for 3 years, they should be replaced at the end of 3 years. Specified maintenance should be completed at the interval stated in the vendor's documentation. This maintenance could include but is not limited to changing filters, cleaning, replacing consumable parts, testing the unit, or checking for worn parts.

All network equipment that is located throughout the casino and not in the computer room must be secured. The method of securing the devices must ensure that an unauthorized individual cannot gain access to the equipment. All network ports must be disabled or secured. This can include a locking case, unplugging the cable from the switch, making the port inaccessible, or logically disabling the port. An inventory of all unused ports must be maintained.