# Global Information Assurance Certification Paper

**Mission Statement**

Viva Casino provides world-class gambling and entertainment facilities in Las Vegas with our primary focus to provide our guests with a safe, secure, and enjoyable experience.

**High Level Security Policy (Security Principles)**

Viva Casino is dedicated to providing a safe and secure gaming environment for our visitors as well as our employees.

We ensure our quality of staff by performing detailed background checks, extensive training once they are on board, and provide processes to ensure all cash transactions and gambling services are performed in accordance with our internal standards.

We provide unequalled safety and security by using state-of-the-art surveillance systems that oversee all gaming and customer areas, direct communication with local law enforcement, and internal communication system allowing for immediate response for any situation.

Viva Casino also complies with all federal and state regulatory agencies that are required by the Nevada Gaming Commission including maintaining are HIPAA and GLB certifications.

**Security Principle**

*Viva Casino is dedicated to providing a safe and secure gaming environment for our visitors as well as our employees.*

**Process Improvement**

Level I

- Provide 24 hour video surveillance and monitoring in all gaming areas and cash locations
- Maintain relationships with local law enforcement by holding regular informal meetings
- Staff security at hotel elevators to verify customers have keys

Level II

- Install video monitoring in all data room access areas. Monitoring will extend from the data center entrances and every area of the data center
- Install environmental sensors and monitoring for fire, camera interference, water, smoke, and motion detection
- Install monitoring in additional areas such as elevators, all exterior perimeter walls, staff areas (such as laundry and maintenance),

basement, and roof
- Provide redundancy for internal communications system

Level III
- Contract with 3rd party to periodically review surveillance data
- Contract with trusted consultants to review security procedures and new security, monitoring, and auditing technology
- Install card reading system with biometrics and UV sensors to monitor staff locations and access
- Install environmental sensors and monitoring for fire, camera interference, water, smoke, and motion sensors
- Install "duress" alert system at every gaming table and with every employee that works on the gambling floor

---

*Issues that may be seen as potentially difficult to implement due to opposition of affected staff*

**Security Model Issue #1**

- *Install card reading system with biometrics and UV sensors to monitor staff locations and access*

**Explanation to Staff**

Due to the nature of the gambling industry, there are those who may come to our casino and lose much than they can afford. Las Vegas has the highest suicide rate per capita which lends itself to people becoming desperate. In order to protect our employees and be able to find all staff members in case of an incident, we are installing a new card reading with sensors to monitor our staff locations. While no one expects something to happen to our employees, we want to be proactive in protecting our employees..

**Why it will work**

We're not telling people that we need to track them because we don't trust them. This new system is being implemented to protect the employee.

**Security Model Issue #2**

- *Contract with 3rd party to periodically review surveillance data*

**Explanation to Staff**

We all know that now that we have 500 cameras keeping track of all

operations, there is not time to see all the taped info. We want you to be focused on what is happening real-time and focusing 100% of your energy doing that. We realize that not all violators are caught watching them real time, as you know, there are new ways of trying to steal everyday. Therefore, we will be having a consultant spend time offsite reviewing taped information. When the consultant finds someone cheating, he will review with all of you what he saw to keep you informed of new ways people are try to cheat.

**Why it will work**

They will be able to learn new techniques of that people use to cheat. This will allow them to be more skilled at what they do. We're not telling the security group that we don't think they are doing a bad job, but that they have so much to watch, they may not see everything or be able to know all the cheating techniques.

**Security Model Issue #3**

- *Contract with trusted consultants to review security procedures and new technology*

**Explanation to Staff**

In order to keep you (security staff) on the cutting edge of security methodologies and equipment, we will be having a consultant review our current methods and equipment to see what tools are now available that will allow us to maintain our excellence and improve our chance rate of violators..

**Why it will work**

By approaching the issue in a positive way, they will be getting even better technology. By nature, security is motivated by being able to catch more people cheating and taking advantage of the casino. At first they may be opposed do to being suspicious, but the vendor will be instructed to begin the consulting engagement by demonstrating the latest technologies (to get the staff excited about the available new technology) and also to address any negative feedback or discovered issues directly with upper management, not to address them with security staff.

---

**Business Continuity for Security Model**

- ***Install card reading system with biometrics and UV sensors to monitor staff locations and access***

Condition:

- Failure of card reader / biometric system

Affect to Operations:

- no one can gain access to staff authorized areas in building
- staff cannot be tracked

Areas Affected:

- Offices, currency areas, back office operations

**Business Continuity Plan**

- System will have override capability with key control to all sensor controlled areas
- System requires 2 unique keys to open sensor doors. Both keys must be inserted into lock before door will open
- All managers on every shift will be assigned with one unique system override key (all manager keys are identical)
- A second unique key (different from the manager key) will be in the possession of the main floor "Pit Boss"
- Override keys will only work with both the manager key and pit boss key inserted concurrently
- This will ensure that no one person can access a sensor door via override keys without another manager present (accountability)
- Managers involved with opening areas will be responsible for access of other staff members into secured areas (credentials will be checked and a log will be maintained by manager monitoring door)
- The sensor system will have redundant power (UPS) and also be on a circuit that has generator power
- Sensor system servers will be distributed (2 distant areas of building)
- Each sensor system server is capable of controlling all areas in case of failure. Each server controls ½ of sensors and be the on-line redundant server (secondary) for the other half.

- In event of sensor failure, a physical count of all staff on shift will be performed by every supervisor to account for all staff on duty during their shift

---

**Risk Management**

**Business Continuity Problem**

- *Install card reading system with biometrics and UV sensors to monitor staff locations and access*

**FMECA Analysis**

**Step 1 - System Mission**

- To allow only those authorized to enter secure areas of the building. This will also track employees to display locations at all times.

**Step 2 - Block Diagram**

- Two servers – located in different areas of the building
- Badge readers
- Ethernet Switches – Located in secured IDF's
- badge

**Step 3 - Individual system module and interface failures**

- Badge to Card Reader
- Card reader to Server
- Server to Server
- Server to Switch
- Badge reader to Switch

**Step 4 – worst case scenario**

| | |
|---|---|
| • Server fails | Critical |
| • Both servers fail | Catastrophic |
| • Badge fails | Minor |
| • Switch fails | Catastrophic |
| • Badge to card reader | Minor |
| • Card reader to server | Critical |
| • Server to server | Marginal |
| • Server to switch | Critical |

- Badge reader to switch Critical

**Step 5 – Identify and Detecting Failures**

- Monitoring
- Logging
- Alerting

**Step 6 – Actions to prevent or eliminate failures**

- Check logs daily, system will page if specified events occur
- Redundant server, splitting load with auto registration with any live server
- Redundant switches, different areas of building
- Spare switch in case any switch fails
- Keep inventory of spare card reader(s) in house
- Standby server hardware and software (cold standby)
- Backup system regularly and main structured backup system
- Lost badges will be deactivated before a new one is issued

**Step 7 – Analyze and describe any effects of additional controls**

- Spare equipment must be maintained to current software versions
- Backup system procedures and policies must be in place to insure quality and availability of tapes
- Policies for issue of badges must be followed
- No one person can create a badge (separation of duties)
- Log of activity and active badge users will be reviewed and signed off my management on a regular basis

**Step 8 – Document the Analysis**

Problems Found in providing a safe, secure, and monitoring of casino activities and crimes include the following

- Lack of technology in security systems
- Lack of controls
- Lack of policy to reduce security risks and increase safety
- Lack of awareness of security policies
- Lack of monitoring of staff access
- Lack of redundancy and ability to perform a “quick recovery” in case of failure of systems.
- Limited separation of duties
- No Principles of Least Privilege in security systems
- No Principle of Complete Mediation in security systems
- Lack of monitoring prevented reaction to solve problems

The solution to the problems

- Technology will be introduced that includes a state-of-the-art

badge, monitoring, and alerting system
- Staff tracking will be installed as part of the badge system
- Policies will be created
- Controls will be put into place that will include
    - Separation of Duties
    - Principle of Least Privilege
    - Complete Mediation
- Logging of all badge access and staff locations will be reviewed regularly, backed up, and be kept offsite for historical record
- Redundancy will be included for all hardware (including network, badge readers, and servers), backups, and service restoration procedures will be maintained and reviewed regularly
- In case of catastrophic failure, a manual backup system has been included.
- Training awareness will be provided and start of employment and refresher training will be required on a regular basis

**Residual Risks**

- Organized Corruption
- Not following policy and procedures
- Individual Corruption

**Impact of Residual Risks**

- Due to the nature of the business, any of the residual risks listed above could result in petty losses and lack of controls to huge monetary losses.
- Corruption that was released to the press could result in a loss of confidence in safety which would result in loss of customers and potential huge monetary losses.