🎰 Casino Revenue Systems
Sarbanes-Oxley (SOX) Compliance Policy
Prepared By: Jose Guerrero
Department: Information Security & Compliance
Version: 1.0
Effective Date: February 9, 2026

---

1. Purpose
The purpose of this policy is to ensure that all systems, processes, and personnel handling financial data within the casino comply with the **Sarbanes-Oxley Act (SOX)**.
This policy establishes:
- Clear responsibilities for financial system management
- Internal controls for accuracy, integrity, and auditability of revenue data
- Procedures for monitoring, reporting, and remediating compliance issues

This policy aligns IT, Finance, and Operations teams to ensure **trustworthy financial reporting and regulatory compliance**.

---

2. Scope
This policy applies to all employees, contractors, and third-party vendors who interact with:
- Slot machine and table game revenue systems
- Player tracking and rewards databases
- Financial reporting and accounting systems
- Supporting IT infrastructure, including servers, networks, and cloud services

All systems that support financial reporting are considered **in-scope for SOX compliance**.

---

3. Roles & Responsibilities
Executive Leadership
- Certify the accuracy of financial reports and ensure internal controls are implemented.

IT Department
- Manage system access and enforce least privilege
- Implement security controls
- Maintain system and audit logs
- Report control status and exceptions to Compliance

Finance & Accounting
- Ensure proper reporting of revenue
- Reconcile financial transactions
- Follow internal control procedures

Compliance Team
- Conduct internal audits
- Review effectiveness of controls
- Report deficiencies to management

All Employees
- Follow access and change management procedures
- Report suspicious activity
- Complete annual compliance training
- Maintain integrity of financial data

---

4. Internal Controls
The casino maintains **IT General Controls (ITGCs)** to safeguard financial data:
ITGC-01 – Role-Based Access Control (RBAC)
- Access granted based on least privilege
- No shared administrator accounts
- Separation between IT and accounting responsibilities
- Periodic access reviews

ITGC-02 – Separation of Duties (SoD)
- No single individual can both approve and modify financial transactions
- System administrators cannot audit their own changes

ITGC-03 – Vulnerability Management
- Continuous monitoring using Tenable Cloud or equivalent

- Critical vulnerabilities remediated according to defined timelines
- Risk reviews conducted regularly

ITGC-04 – Patch Management

- Security patches applied in a timely manner
- Critical patches applied immediately
- Emergency patching process documented

ITGC-05 – Logging & Audit Trails

- All financial system activity is logged: logins, privileged commands, database changes, and configuration changes
- Logs retained for a minimum of 7 years
- Logs stored in a tamper-resistant repository

---

5. Change Management

All changes to financial reporting systems, revenue databases, and supporting IT infrastructure must:

- Be formally requested and documented
- Be reviewed and approved prior to deployment
- Be tested in a non-production environment before implementation
- Be logged for audit purposes

Unauthorized changes are prohibited and considered a **SOX violation**.

---

6. Daily Compliance Monitoring

Compliance and IT teams perform automated and manual monitoring to:

- Verify privileged access controls
- Confirm vulnerability monitoring systems are operational
- Review authentication and system logs
- Track patch status and remediation progress
- Retain evidence for audits

Daily findings are documented and reported to the compliance manager.

---

7. Training & Awareness

- All employees complete mandatory **annual SOX compliance training**
- Training includes internal controls, access management, change procedures, and incident reporting
- Refresher courses provided when systems change or issues are identified
- Completion is tracked by the compliance team

---

8. Incident Reporting & Control Failures

If a control failure or potential compliance violation occurs:

1. Document the issue immediately
2. Assess risk and impact on financial reporting
3. Assign remediation responsibility
4. Notify executive leadership if material
5. Retest the control after remediation
6. Retain evidence for audit purposes

Significant deficiencies must be disclosed in accordance with SOX Section 404.

---

9. Enforcement & Consequences

Violations of this policy may result in:

- Disciplinary action, up to and including termination
- Regulatory penalties
- Mandatory remediation training

Employees are responsible for reporting violations through established channels.

---

10. Policy Review

This policy will be reviewed **annually** or when:

- Significant changes occur to financial systems
- Internal or external audits identify control issues
- SOX regulations are updated

The compliance department maintains and communicates this policy.