GLI®

GAMING SECURITY FRAMEWORK

GLI-GSF-4

GAMING INFORMATION SECURITY (GIS) AUDIT – LANDBASED GAMING CONTROLS

Version 1.0 – Published September 30, 2025

GAMING LABORATORIES INTERNATIONAL®

Contents

1. INTRODUCTION

1.1. General Statement

The integrity and accuracy of the operation of a Gaming Production Environment (GPE) is highly dependent upon operational procedures, configurations, and the network infrastructure. With ever emerging threats to gaming operations, Regulatory Bodies rely heavily on the expertise of a qualified Independent Security Firm (ISF) to perform gaming security assessments as an essential addition to the testing and certification of the Critical System Components of a GPE by an Independent Test Laboratory (ITL).

a. This module of the GLI Gaming Security Framework, GLI-GSF-4, establishes the additional Gaming Information Security (GIS) Controls to the GLI-GSF-1, which are necessary for auditing a Gaming Enterprise's Gaming Information Security Management System (GISMS) to ensure effective management of security in a Gaming Enterprise's GPE used in landbased gaming operations, such as a casino, gaming hall, racetrack, or other physical gaming venue or location, which offers gaming devices, table games, bingo, lottery, event wagering, or any other form of landbased gaming.
b. This module is intended to be evaluated as a companion to the GLI-GSF-1, which provides the common GIS Controls necessary for auditing a Gaming Enterprise's GISMS.
c. This module may be used alongside the GLI-GSF-2, which provides a benchmark for conducting Gaming Technical Security (GTS) assessments of a Gaming Enterprise's GPE.
d. Depending on the type of Gaming Enterprise, additional modules of the GLI-GSF may also apply.

NOTE: The entire GLI Gaming Security Framework (GLI-GSF) is available free of charge at www.gaminglabs.com.

1.2. Gaming Enterprise and Sensitive Data Management Role

Ensuring the security of a GPE is a collective responsibility that spans across the multiple entities which make up the Gaming Enterprise, such as the operator, and its suppliers, manufacturers, vendors, service providers, and other entities who have a role in overseeing or the operation of a GPE or providing services integral to its function. Each entity plays a crucial role in maintaining the confidentiality, integrity, availability, and accountability of the environment, especially when sensitive data is involved. For additional information, please refer to the "Gaming Enterprise and Sensitive Data Management Role" section of the GLI-GSF-1.

NOTE: This document is not intended to define which entities are responsible for meeting each GIS Control. It is the responsibility of the multiple entities which make up the Gaming Enterprise to agree on responsibility.

1.3. Gaming Production Environment (GPE)

A GPE refers to the operational setting where landbased gaming activities and related services are conducted, managed, and delivered to patrons in a live or real-time manner. It encompasses the physical and virtual infrastructure, gaming systems, software, and processes required to facilitate various forms of landbased gaming, such as live and electronic gaming, retail lottery, and retail event wagering. The GPE also encompasses the backend systems, business applications, and infrastructure that interface and/or support landbased gaming activities. Key characteristics of a GPE are described in the "Gaming Production Environment (GPE)" section of the GLI-GSF-1.

1.4. Gaming Information Security Management System (GISMS)

A GISMS is a structured framework and set of processes designed to safeguard a Gaming Enterprise's sensitive data, assets, and Critical System Components within its GPE against unauthorized access, disclosure, alteration, or destruction. It encompasses policies, procedures, controls, and risk management practices specifically tailored to the unique challenges and regulatory requirements of the gaming industry by involving the identification of GIS risks, the implementation of appropriate controls and safeguards, ongoing monitoring and assessment of security measures, and continuous improvement to adapt to evolving threats and compliance requirements.

1.5. Framework Purpose

Ensuring the security and integrity of landbased gaming activities is paramount for upholding public confidence and trust in the sector. Therefore, Gaming Enterprises offering landbased gaming must establish and uphold a clearly defined and documented framework to attain and preserve public trust in their operations. The goal is to align GIS in such a way that gaming operations can function as other eCommerce operations to ensure a safe and stable environment with the secure features of operations in parallel industries.

1.6. Security Standards and Guidelines Consulted

Each module of the GLI-GSF is based on commonly used security standards and guidelines that provide an industry-accepted foundation developing effective GIS management practices. GLI acknowledges and thanks the Regulatory Bodies and other industry participants who have assembled rules, regulations, technical standards, and other documents which have been influential in the development of this document.

1.7. Adoption and Observance

This module of the GLI-GSF may be adopted in whole or in part by any Regulatory Body that wishes to implement a comprehensive set of GIS Controls to be applied for landbased gaming in conjunction with Common GIS Controls from the GLI-GSF-1.

2. LANDBASED GIS (LGIS) CONTROLS AUDITS

2.1. Audit Overview

The LGIS Controls Audit is performed with the intent of identifying any actual or potential instances of non-compliance, vulnerabilities, or weaknesses, and assuring that the confidentiality, integrity, availability, and accountability of the information under the Gaming Enterprise's control are preserved. This methodology relies heavily on layered security to reduce the risk to computer and network systems by providing redundancy and reinforcing the overall security model, as several layers of security must be breached before a sensitive data store is accessed.

NOTE: The focus of the GIS guidance detailed in the GLI-GSF-4 is on specific information security controls for landbased gaming to apply in addition to the common information security controls for gaming in GLI-GSF-1, other evaluation methods are discussed in supporting modules of the GLI-GSF.

2.2. Audit Methods

The LGIS Controls Audit uses a range of assessment methods including the following methods, the results of which are used to support the determination of LGIS Control effectiveness over time:

a. Interview: A type of assessment method characterized by the process of conducting discussions with individuals or groups within a Gaming Enterprise to facilitate understanding, achieve clarification, or lead to the location of evidence.
b. Examine: A type of assessment method characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.
c. Test: A type of assessment method characterized by the process of exercising one or more audit objects under specified conditions to compare actual with expected behavior.

2.3. Audit Tasks

The Appendix details the minimum LGIS Controls in more granular detail. Users of this document are directed to the Appendix of this module as well as the Appendix of the GLI-GSF-1 to ensure that no necessary GIS Controls are overlooked. The LGIS Controls listed in the Appendix are not exhaustive and in addition to the common GIS Controls from the GLI-GSF-1, additional GIS Controls may be included based on regulatory requirements and scope of the assessment.

NOTE: Information on the high-level LGIS Controls Audit activities can be found within the "Audit Tasks" section in the GLI-GSF-1, including, but not limited to documentation review, interviews, controls assessment, GIS incident response plan assessment, and risk assessment.

2.4. Audit Frequency

LGIS Controls Audits must be performed by an ISF with the "Audit Frequency" expressed within the GLI-GSF-1. This may include additional audits as requested by the Regulatory Body or Gaming Enterprise, focused specifically on critical changes within the GPE that could affect the security of the GPE, that could allow access to sensitive data and/or Critical System Components, or any other changes impacting data flow or security posture.

NOTE: The Regulatory Body or Gaming Enterprise may also request a Vulnerability Scan or Gaming Technical Security (GTS) Testing be performed specifically on the critical changes and the Critical System Components affected by the changes. Please refer to GLI-GSF-2 for additional information.

2.5. Audit Reports

The results of a LGIS Controls Audit identify for Gaming Enterprises those areas in the operations where improvement should be considered and recommend strategies for improving those areas. The LGIS Controls Audit report must meet the requirements for "Audit Reports" as specified in the GLI-GSF-1.

2.6. Remediation

If the ISF's LGIS Controls Audit report recommends remediation, the Gaming Enterprise must provide the Regulatory Body and the ISF, if required by the Regulatory Body, with a remediation plan and any risk mitigation plans which detail the Gaming Enterprise's actions and schedule to implement the remediation steps.

NOTE: For additional information, please refer to the "Remediation" section of the GLI-GSF-1.

2.7. Independent Security Firm (ISF)

The LGIS Controls Audit must be carried out by individuals with sufficient qualifications, which means that the ISF must employ sufficiently qualified, competent, and experienced individuals. Unless otherwise specified by the Regulatory Body, these individuals must meet the qualifications specified for an "Independent Security Firm (ISF)". in the GLI-GSF-1.

APPENDIX: LANDBASED GAMING INFORMATION SECURITY (GIS) CONTROLS

In addition to the Common GIS Controls specified in the GLI-GSF-1 for GIG1, GIG2, or GIG3 Gaming Enterprises (as applicable), the following additional GIS Controls apply to Gaming Enterprises' GPEs offering landbased gaming.

LGIS-1	**Integrity Verification of Critical System Components**
LGIS-1.1	**Software, Hardware, and Configuration Integrity Verification**
LGIS-1.1.1	Documented procedures must be established and implemented to periodically and on-demand verify that critical control programs, hardware components, and significant configurations are authentic, unaltered, and identical to the versions certified by an approved Independent Test Laboratory and authorized by the regulatory body.
LGIS-1.1.2	Verification procedures must be based on risk assessments and clearly specify tools, responsible personnel, and documentation requirements.
LGIS-1.1.3	Verifications must occur at defined intervals such as upon initial installation, after any critical control programs or other critical system component replacement, after significant maintenance, periodically as defined by risk assessment (e.g., daily or weekly for critical parameters), and on demand by designated personnel.
LGIS-1.2	**Verification Audit Log**
LGIS-1.2.1	All integrity verification activities must be recorded in a verification audit log which must be accessible by the Regulatory Body on demand.
LGIS-1.2.2	The verification audit log must detail the following for each signature verification: a. The date and time of the verification; b. Description of the components or configurations verified; c. Details of any discrepancies or failures detected; d. Corrective actions taken and resolution status; and e. Identity of individual initiating the verification procedure when performed on demand.
LGIS-1.3	**Verification Failure**
LGIS-1.3.1	Any failure of integrity verification of any Critical Control Program must require a notification of the verification failure to be communicated to the Gaming Enterprise.
LGIS-1.3.2	Where required by the Regulatory Body, the Gaming Enterprise must report any failures in integrity verification activities and corrective actions taken to the Regulatory Body without undue delay.
LGIS-2	**System Procedures**
LGIS-2.1	**Detection and Response to Master Reset Events**
LGIS-2.1.1	The Gaming Enterprise must establish controls to detect, identify, and properly respond to any occurrence of a master reset on a Critical System Component.
LGIS-2.1.2	The master reset event must be logged with a timestamp, including relevant Critical System Component identification and user context.
LGIS-2.2	**Copy Protection**
LGIS-2.2.1	Copy protection to prevent unauthorized duplication or modification of licensed software, including Critical Control Programs may be implemented provided that: a. The method of copy protection is fully documented and can be verified that the protection works as described; or b. The program or component involved in enforcing the copy protection can be individually verified by the methodology approved by the Regulatory Body.
LGIS-3	**Information Technology (IT) Personnel**
LGIS-3.1	**Segregation of Duties**
LGIS-3.1.1	IT Personnel must be operationally independent from gaming-related functions within the Gaming Venue, including at minimum, separation of duties, reporting lines, and access controls.
LGIS-3.1.2	GIS policies and documented procedures must be implemented to ensure adequate functional separation between IT Personnel and those responsible for financial or gaming operations.
LGIS-3.1.3	The GIS policies and documented procedures must include, but are not limited to: a. Logical and physical access restrictions; b. Role-Based Access Controls (RBAC); and c. Monitoring, audit trails, and access reviews.

LGIS-3.2	**IT Personnel Responsibilities and Restrictions**
LGIS-3.2.1	All IT responsibilities and restrictions must be formally documented in written procedures, with roles and duties communicated to relevant personnel and reviewed periodically.
LGIS-3.2.2	IT Personnel must be restricted from: a. Accessing or handling financial instruments (e.g., cash, wagering instruments, or equivalents) or liquid financial assets in any form; b. Accessing and revising accounting records and audit documentation; c. Initiating, authorizing, or approving entries in general or subsidiary ledgers; and d. Accessing payout forms or other instruments representing patron value.
LGIS-3.2.3	IT Personnel may not have signatory authority over: a. Financial instruments (e.g., cash, wagering instruments, or equivalents); and b. Payout forms or other instruments representing player value.
LGIS-3.2.4	IT Personnel must be precluded from unauthorized access to the following: a. Server consoles and user terminals located within the gaming areas; b. Source documents (e.g., original accounting records); and c. Live production data files, except where specifically authorized for testing or troubleshooting.
LGIS-3.2.5	IT Personnel access to test data in non-production environments is permitted under controlled conditions established by the Gaming Enterprise.
LGIS-4	**Secured Server Areas and Data Closets**
LGIS-4.1	**Physical Security of Components and Infrastructure**
LGIS-4.1.1	All locally installed Critical Control Components and non-gaming IT infrastructure shall be housed within a secured server area and data closets inside the Gaming Venue.
LGIS-4.1.2	The secure server area and data closets must be physically secured to prevent unauthorized access, environmental damage, and interruption of service.
LGIS-4.1.3	The secure server area and data closets must be located away from areas with high risks of physical damage or unauthorized observation.
LGIS-4.1.4	Cables within the secure server area and data closets must be maintained properly and protected from both environmental hazards and possible interference.
LGIS-4.2	**Surveillance of Secured Server Areas and Data Closets**
LGIS-4.2.1	Surveillance systems must provide coverage for not only the gaming area but also the secured server area and data closets and all methods to access the secured server area and data closets.
LGIS-4.2.2	Where surveillance coverage is impractical the Gaming Enterprise may consider allowing compensating controls such as restricted key card access logs.
LGIS-5	**Physical Access Controls**
LGIS-5.1	**Access Restrictions and Authorization**
LGIS-5.1.1	Access to the secured server area and data closets shall be restricted strictly to authorized personnel, as defined in the Gaming Enterprise's formal access control policies and procedures.
LGIS-5.1.2	Authorization must be role-based and limited to operational necessity.
LGIS-5.1.3	The Gaming Enterprise shall maintain an up-to-date access log or record of all personnel granted secured server area access privileges.
LGIS-5.2	**Access Device Control**
LGIS-5.2.1	Access devices (e.g., magnetic swipe, proximity cards, embedded chip cards) used to enter the secured server area or data closets must be: a. Uniquely numbered and assigned; and b. Controlled and managed by personnel independent of IT operations and gaming functions.
LGIS-5.2.2	The Gaming Enterprise must maintain documentation of each type of access device, its functions, and the job positions authorized to be assigned and use that access device.
LGIS-5.2.3	The responsibility for issuance, revocation, and auditing of access devices must be clearly assigned in the GIS Policy.
LGIS-5.2.4	Each access device must only be: a. Assigned to personnel who need the access device to perform their job duties; and b. Utilized by the personnel to whom the access device is assigned.
LGIS-5.2.5	The Gaming Enterprise must maintain a list of all access devices numbers and the personnel assigned to each access device.
LGIS-5.2.6	Any access device that could be used at multiple Gaming Venues must be treated as a sensitive key.

LGIS-6	Logical Access Controls
LGIS-6.1	**Integration of Logical Access Controls**
LGIS-6.1.1	Logical access controls must be implemented to complement and reinforce physical security measures. Logical access controls include, but are not limited to: a. User authentication (e.g., unique user account IDs, strong passwords, biometrics, multi-factor authentication, etc.); b. Role-Based Access Control (RBAC) aligned with least privilege principles; c. System and network segmentation to restrict unauthorized pathways; d. Audit logging and monitoring of access attempts and activities; and e. Automated alerting for unauthorized access or anomalous behavior.
LGIS-6.1.2	Logical access controls shall ensure that only authorized personnel are able to access the locally installed Critical Control Components and non-gaming IT infrastructure.
LGIS-6.2	**Automated Equipment Identification**
LGIS-6.2.1	When employed, automated equipment identification methods, such as MAC address filtering, device certificates, hardware security tokens, or other cryptographic techniques, must be used to authenticate connections from specific equipment and locations.
LGIS-6.2.2	The automated equipment identification mechanisms must: a. Be fully documented, including the identification method, the authorized equipment, and associated access rights; b. Be integrated into the organization's logical access control procedures; c. Be included in periodic reviews of user access rights and system privileges to ensure that access remains appropriate and authorized; and d. Support non-repudiation by associating system access with both the authenticated user and the verified equipment.
LGIS-6.3	**Automatic Session Locking and Security**
LGIS-6.3.1	Server consoles, workstations, user terminals, portable electronic devices (e.g., electronic tablets or other portable terminals), or kiosks within a Gaming Venue must automatically secure themselves after a defined period of inactivity to prevent unauthorized access.
LGIS-6.3.2	The methods and procedures for automatic session locking, for each type of device, must be delineated within the GIS Policy, and include at a minimum: a. The period of inactivity as determined by management defined by risk assessment; b. For portable electronic devices and kiosks: i. The system functions and/or applications which are available or can be accessed on or through each device or kiosk; ii. The controls over user access to the system functions and applications; iii. The procedures utilized to secure the network when such devices or kiosks are in use; and c. For portable electronic devices, the controls over the physical safeguarding and distribution of such devices.
LGIS-7	**Remote Access to Installed Equipment, Systems, and other Components**
LGIS-7.1	**Vendor Remote Access**
LGIS-7.1.1	Vendor remote access to Electronic Gaming Equipment, Gaming Systems, and other Critical System Components installed in the Gaming Venue must be restricted.
LGIS-7.1.2	Multi-factor authentication must be used if vendor remote access is required for maintenance or administration purposes.
LGIS-7.1.3	Remote access methods must be maintained, controlled, and monitored by the Gaming Enterprise, not the Vendor.
LGIS-7.2	**Remote Dial-Up**
LGIS-7.2.1	If remote dial-up to the Electronic Gaming Equipment, Gaming Systems, and other Critical System Components is allowed for software support, the gaming operation must maintain an access log that includes: a. Name of employee authorizing remote access; b. Name of authorized programmer or Service Provider representative; c. Reason for remote access; d. Description of work performed; and e. Date, time, and duration of access.

LGIS-8	Gaming Venue Network Security
LGIS-8.1	**Connectivity**
LGIS-8.1.1	Only authorized equipment must be permitted to establish communications between any Critical System Components.
LGIS-8.1.2	The Gaming Enterprise must provide a method to a. Perform mutual authentication to ensure that authorized equipment only communicate with valid networks; b. Enroll and un-enroll Critical System Components; and c. Enable and disable specific Critical System Components.
LGIS-8.1.3	Only enrolled and enabled Critical System Components may participate in gaming operations.
LGIS-8.1.4	The default condition for Critical System Components must be un-enrolled and disabled.
LGIS-8.1.5	The establishment, loss, and reestablishment of communications between Critical System Components must be recorded in an audit log.
LGIS-8.2	**Electronic Gaming Equipment Connection Security**
LGIS-8.2.1	Electronic Gaming Equipment must not be connected to their respective Gaming Systems via insecure or unauthorized network connections.
LGIS-8.2.2	Regular audits of Electronic Gaming Equipment network connections and configurations must be performed.
LGIS-8.2.3	Any deviation from approved connection methods must be documented and justified.
LGIS-8.3	**Network Segmentation**
LGIS-8.3.1	The gaming network, encompassing all Electronic Gaming Equipment, Gaming Systems, and other Critical System Components, must be logically and/or physically separated (segmented) from corporate/business networks, guest networks, and any other non-gaming networks within the Gaming Venue.
LGIS-8.3.2	The Gaming Enterprise must implement Virtual Local Area Networks (VLANs) for logical segmentation and consider separate physical switches for highly critical segments.
LGIS-8.3.3	All communication paths between the gaming network and any non-gaming network must be explicitly documented (detailing source, destination, ports, protocols, and business justification), approved by IT management, and strictly controlled through appropriately configured firewalls or other suitable boundary protection devices adhering to a implicit-deny security posture.
LGIS-8.4	**Access Ports and Data Port Protection**
LGIS-8.4.1	Wireless access points (WAPs), wired data ports (WDPs), and other publicly accessible locations in the Gaming Venue that provide network connectivity must be physically/logically secured or disabled if not in use.
LGIS-8.4.2	Active WAPs and WDPs must be controlled by Network Admission Control (NAC) port security, or equivalent mechanism to prevent unauthorized device connections (e.g., 802.1X authentication, MAC filtering, etc.).
LGIS-8.4.3	WAPs and WDPs must be located to minimize opportunities for unauthorized direct physical access by the general public.
LGIS-8.4.4	Physical locks, tamper-evident seals, or port blockers must be used on unused WDPs.
LGIS-8.4.5	Surveillance system must provide coverage for WAPs, WDPs, and other publicly accessible locations in the Gaming Venue that provide network connectivity.

DEFINITIONS OF TERMS

Term	Descriptions
Access	Ability to make use of any GPE resource.
Access Control	The process of granting or denying specific requests for obtaining and using sensitive data and related services specific to a system; and to enter specific physical facilities which houses critical network or system infrastructure.
Application	Computer software that is designed to help a user perform a specific task.
Audit Log	An auditable record of actions, events, or changes within a GPE, capturing details such as user activities, access attempts, alterations, and system operations to ensure security, compliance, and accountability during a given period.
Authentication	Verifying the identity of a user, process, software package, or device, often as a prerequisite to allowing access to resources in the GPE.
Authentication Credentials	Any passwords, multi-factor authentication, digital certificates, PINs, biometrics, security questions and answers, and any other account access methods (e.g., magnetic swipe, proximity cards, embedded chip cards).
Availability	Ensuring timely and reliable access to and use of information.
Biometrics	A biological identification input, such as fingerprints, retina patterns, facial recognition data, or voiceprints.
Business Applications	Applications operating as a shared service for users to collect, process, maintain, use, share, disseminate, or dispose of sensitive data within the GPE for compliance auditing and GIS incident response purposes.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Critical Control Program	Software programs that control behaviors relative to any applicable technical standard and/or regulatory requirement, such as executables, libraries, gaming or system configurations, operating system files, components that control required system reporting, and database elements that affect gaming or system operations.
Critical System Component	Any hardware, software, critical control programs, communications technology, other equipment or components implemented in a GPE to allow patron participation in gaming, and whose failure or compromise can lead to loss of patron entitlements, government revenue or unauthorized access to data used for generating reports for the Regulatory Body. Examples of Critical System Components include, but are not limited to: • Components which record, store, process, share, transmit, or retrieve sensitive data. • Components that could impact the security of sensitive data or the GPE. • Components which generate, transmit, or process random numbers used to determine the outcome of games and events. • Components which store results or the current state of a patron's game, wager, or available funds. • Points of entry to and exit from the above components, including other systems which communicate directly with Critical System Components. • Communications technology and networks which transmit sensitive data, including network communication equipment (NCE) and network security controls. • Components that provide security services, including authentication servers, access control servers, security information and event management (SIEM) systems, physical security systems, surveillance systems, multi-factor authentication (MFA) systems, anti-malware/anti-virus systems. • Components that facilitate segmentation, including internal network security controls.

Term	Descriptions
	• Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. • Cloud infrastructure and components, both external and on premises, and including instantiations of containers or images, virtual private clouds, cloud-based identity and access management, components residing on premises or in the cloud, service meshes with containerized applications, and container orchestration tools. • Server types including web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name Service (DNS). • End-user devices, such as computers, laptops, workstations, administrative workstations, tablets, and mobile devices. • Applications, software, and software components, serverless applications, including all purchased, subscribed (e.g., Software-as-a-Service), custom, and in-house built applications, including internal and external (e.g., Internet) applications. • Tools, code repositories, and systems that implement software configuration management or for deployment of objects to the GPE or to components that can impact the GPE. • Corporate networks and systems that interface with the GPE and from which attackers could use to move laterally into the GPE (e.g., corporate casinos' networks and online operators' corporate networks). • Any other component deemed critical to the GPE by the Regulatory Body or the Gaming Enterprise.
Electronic Gaming Equipment	A gaming device, electronic table game, electronic wager station, live game management component, lottery terminal, wagering device, kiosk, or any other critical electronic gaming component and its Interface Element intended for use with a Gaming System.
Encryption	The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people. Where encryption is not possible due to a technology or performance limitation, other reasonable protective measures must be implemented in its place and reviewed on a case-by-case basis.
Firewall	A component of a computer system or network that is designed to block unauthorized access or traffic while still permitting outward communication.
Gaming Enterprise	An operator, and any suppliers, manufacturers, vendors, service providers, and/or other entities who have a role in overseeing the operation of a GPE, or providing services integral to its function, including the management of sensitive data.
Gaming Information Security (GIS)	Protecting sensitive data and Critical System Components from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, availability, and accountability.
Gaming Information Security Management System (GISMS)	A defined, documented management system that consists of a set of policies, processes, and systems to manage risks to a Gaming Enterprise's sensitive data, assets, and Critical System Components within a GPE, with the objective of ensuring acceptable levels of GIS risk.
Gaming Production Environment (GPE)	The operational setting where gaming activities and related services are conducted, managed, and delivered to patrons in a live or real-time manner. It encompasses the physical and virtual infrastructure, gaming systems, software, and processes required to facilitate various forms of gaming and/or manage sensitive data, as well as the backend systems and infrastructure that interface and/or support gaming activities.
Gaming Systems	Critical System Components that are relative to any applicable technical standard and/or regulatory requirement for gaming activities.
GIS Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, availability, or accountability of a GPE or the sensitive data the GPE processes, stores, or transmits or that constitutes a violation or imminent

Term	Descriptions
	threat of violation of security policies, security procedures, or acceptable use policies. Examples of reportable GIS incidents include, but are not limited to: • Unauthorized access to sensitive data or Critical System Components. • Malicious code execution or ransomware infection within the GPE. • Loss, theft, or unauthorized disclosure of PII. • System outages or disruptions affecting the integrity or availability of gaming operations for a defined period (e.g., more than 15 minutes). • Detection of tampering, manipulation, or attempted compromise of gaming software or hardware. • Repeated or systemic failed login attempts indicative of a brute-force attack. • Compromise or misuse of administrative credentials or security certificates. • Security configuration changes that were made outside of authorized change management processes.
GIS Incident Response Plan	The documentation of a predetermined set of instructions or procedures when a malicious cyberattack is encountered against a Gaming Enterprise's GPE.
GIS Policy	A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.
Information Technology Personnel (IT Personnel)	Personnel who have access to locally installed Critical System Components and non-gaming IT infrastructure within a Gaming Venue.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Key	A value used to control cryptographic functions, such as encryption, decryption, signatures, hashing, etc.
Layered Security	A defense approach that uses multiple independent protections across a system, like firewalls, authentication, encryption, and monitoring, so that an attacker must bypass several layers before accessing sensitive data or Critical System Components.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, availability, or accountability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Message Authentication	A security measure designed to establish the authenticity of a message by means of an authenticator within the transmission derived from certain predetermined elements of the message itself.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Multi-Factor Authentication (MFA)	A type of authentication which uses two or more of the following to verify a user's identity: • Information known only to the user (e.g., a password, PIN, or answers to security questions); • An item possessed by a user (e.g., an electronic token, physical token, or an identification card); and • A user's biometric data (e.g., fingerprints, retina patterns, facial recognition data, or voiceprints).
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Personally identifiable information (PII)	Sensitive data that could potentially be used to identify a particular person. Examples include a legal name, date of birth, place of birth, government identification number (social security number, taxpayer identification number, passport number, or equivalent), personal financial information (credit or debit instrument numbers, bank account numbers, etc.), or other personal information if defined by the Regulatory Body.

Term	Descriptions
Personal Identification Number (PIN)	A numerical code associated with an individual which allows secure access to a domain, account, network, system, etc.
Port	A physical entry or exit point of a module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).
Protocol	A set of rules and conventions that specify information exchange between devices, through a network or other media.
Regulatory Body	The governmental body or equivalent which regulates or controls the operations of gaming.
Remote Access	Any access from outside the system or system network including any access from other networks within the same site or venue.
Risk	The likelihood of a threat being successful in its attack against a network or system within the GPE.
Risk Assessment	Identifying, analyzing, and prioritizing threats and vulnerabilities to a Gaming Enterprise's operations or assets, or to individuals or other entities, resulting from impairment of the confidentiality, integrity, availability, and accountability of sensitive data or the reliability, security, or capacity of the GPE.
Secured Server Area	IT server room, telecommunications room, and other dedicated space in a Gaming Venue which house Critical System Component and non-gaming IT infrastructure.

Sensitive Data	Information that needs to be handled in a secure manner, including but not limited to, as applicable:
	• Audit logs and system databases recording information used to determine outcome, payment, redemption, and the tracking of patron information;
	• Accounting and significant event information related to the Critical System Components of the GPE;
	• RNG seeds and any other information which affects outcomes of games and wagers;
	• Encryption keys, where the implementation chosen requires transmission of keys;
	• Validation numbers associated with patron accounts, wagering instruments, and any other gaming transactions;
	• Transfers of funds to and from patron accounts, electronic payment accounts, and for the purposes of gaming;
	• Software packages within the GPE;
	• Any location data related to employee or patron activity (e.g. account management, online gaming, etc.);
	• Any of the following information recorded for any employee or patron:
	  • Government identification number (social security number, taxpayer identification number, passport number, or equivalent);
	  • Personal financial information (credit or debit instrument numbers, bank account numbers, etc.);
	  • Authentication credentials in relation to any user account or patron account
	  • Any other personally identifiable information (PII) which needs to be kept confidential; and
	• Any other data deemed sensitive by the Regulatory Body or the Gaming Enterprise.

Server	A running instance of software that is capable of accepting requests from clients, and the computer that executes such software. Servers operate within a Client-Server Architecture, in which “servers” are computer programs running to serve the requests of other programs (“clients”).
Service Providers	Entities that offer platforms, software, and services to Gaming Enterprises. Examples include IT consultants, managed service provider, Software as a Service (SaaS) platforms, and cloud service providers. Third-party providers and vendors are also considered Service Providers.

Term	Descriptions
Signature Verification	Ensuring by electronic signature checking that any software package is an authentic copy of the software created by its manufacturer and, if applicable, an exact copy of the software as certified by the Independent Test Laboratory (ITL).
Switch	Connects devices on an IEEE 802.3 network. A switch forwards data to its destination by using the MAC address embedded in each packet.
Threat	Any circumstance or event with the potential to adversely impact network operations (including mission, functions, image, or reputation), assets, or individuals through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service; the potential for a threat-source to successfully exploit a particular vulnerability; any potential danger to a network that someone or something may be able to identify as being vulnerable, and therefore seek to exploit.
Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
Virus	A self-replicating program, typically with malicious intent, that runs and spreads by modifying other programs or files.
Vulnerability	Software, hardware, or other weaknesses in a network or system that can provide a “door” to introducing a threat.
Wireless Access Point (WAP)	Provides network capabilities to wireless network devices. A WAP is often used to connect to a wired network, thereby acting as a link between wired and wireless portions of the network.
Workstation	An interface for authorized personnel to access the regulated functions of the GPE.