GLI®

GAMING SECURITY FRAMEWORK

GLI-GSF-1

GAMING INFORMATION SECURITY (GIS) CONTROLS AUDIT

Version 1.0 – Published February 7, 2025

Contents

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

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-1, establishes the common Gaming Information Security (GIS) Controls necessary for auditing a Gaming Enterprise's Gaming Information Security Management System (GISMS).
b. These common GIS Controls apply to GPEs used for all forms of gaming, such as casino gaming, lottery, event wagering, and interactive gaming.
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 integrity, availability, and confidentiality of the environment, especially when sensitive data is involved, which at a minimum consists of the following, as applicable:

a. Audit logs and system databases recording information used to determine outcome, payment, redemption, and the tracking of patron information;
b. Accounting and significant event information related to the Critical System Components of the GPE;
c. RNG seeds and any other information which affects outcomes of games and wagers;
d. Encryption keys, where the implementation chosen requires transmission of keys;
e. Validation numbers associated with patron accounts, wagering instruments, and any other gaming transactions;
f. Transfers of funds to and from patron accounts, electronic payment accounts, and for the purposes of gaming;
g. Software packages within the GPE;
h. Any location data related to employee or patron activity (e.g. account management, online gaming, etc.);
i. Any of the following information recorded for any employee or patron:
    i. Government identification number (social security number, taxpayer identification number, passport number, or equivalent);
    ii. Personal financial information (credit or debit instrument numbers, bank account numbers, etc.);
    iii. Authentication credentials in relation to any user account or patron account;
    iv. Any other personally identifiable information (PII) which needs to be kept confidential; and
j. Any other data deemed sensitive by the Regulatory Body or the Gaming Enterprise.

NOTE: This document is not intended to define which entities are responsible for ensuring GIS. 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 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, systems, software, and processes required to facilitate various forms of gaming, such as casino gaming, lottery, event wagering, and interactive gaming. The GPE also encompasses the backend systems, business applications, and infrastructure that interface and/or support gaming activities. Key characteristics of a GPE include:

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

a. Critical System Components: This includes the network devices, servers, computing devices, virtual components, hardware, and software platforms that support the execution of gaming activities, such as gaming devices, gaming tables, gaming systems, lottery systems, event wagering systems, and interactive gaming systems or applications.
b. Cryptographic Modules: Cryptographic modules used within the GPE are responsible for cryptographic functions, including the encryption and decryption of sensitive data, using algorithms which meet current industry accepted standards, such as ISO/IEC 19790, FIPS 140-2, or equivalent.
c. Transaction Processing: The GPE processes monetary transactions related to gaming activities, including wagers, payouts, deposits, withdrawals, and financial transactions with patrons.
d. Security Measures: Robust security measures are implemented to safeguard the integrity, confidentiality, and availability of Critical System Components, sensitive data, financial transactions, and patron information against unauthorized access, fraud, manipulation, and cyber threats.
e. Risk Management: The GPE employs risk management practices to identify, assess, mitigate, and monitor risks associated with gaming operations, including operational risks, financial risks, regulatory risks, and technological risks.
f. Continuous Operation: A GPE typically operates 24/7 to meet patron demand and maximize revenue generation. This requires high availability, reliability, and resilience of infrastructure and systems to minimize downtime and disruptions.
g. Monitoring and Control: Real-time monitoring, surveillance, and control mechanisms are in place to oversee gaming activities, detect anomalies, ensure compliance with rules and regulations, and respond promptly to GIS incidents, fraud, or other issues.
h. Regulatory Compliance: Compliance with gaming regulations, licensing requirements, and industry standards is essential in a GPE to ensure fair play, patron protection, responsible gaming practices, and adherence to legal and regulatory obligations.

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 gaming activities is paramount for upholding public confidence and trust in the sector. Therefore, casinos, lotteries, event wagering operations, interactive gaming operations, and other Gaming Enterprises 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 was 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 Common GIS Controls.

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

2. GIS CONTROLS AUDITS

2.1. Audit Overview

The GIS Controls Audit is performed with the intent of identifying any actual or potential instances of non-compliance, vulnerabilities, or weaknesses, and assuring that the integrity, confidentiality, and availability 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-1 is on common information security controls for gaming, other evaluation methods are discussed in supporting modules of the GLI-GSF.

2.2. Audit Methods

A GIS Controls Audit uses a range of assessment methods including the following methods, the results of which are used to support the determination of GIS 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 following are the high-level GIS Controls Audit activities suggested. The Appendix details the minimum common GIS Controls in more granular detail. Users of this document are directed to the Appendix to ensure that no necessary GIS Controls are overlooked. The GIS Controls listed in the Appendix are not exhaustive and additional GIS Controls may be included based on regulatory requirements and scope of the assessment.

2.3.1. Submitted Documentation Review

The ISF first evaluates the Gaming Enterprise's existing GIS Controls by collecting and reviewing relevant documentation to better understand and assess pertinent aspects of the GPE in relation to overall GIS, and to determine if the documentation adequately complements the technical controls. An example of some of the documentation expected to be reviewed includes, but is not limited to:

a. GIS policy
b. User access
c. Development and testing procedures
d. Service Level Agreement
e. Policy on use of network services
f. Detection, prevention, and recovery controls to protect against malicious code
g. Data backup policy
h. Procedures in place so that media is disposed of securely and safely
i. Procedures for the handling and storage of information (to protect the information from unauthorized disclosure or misuse)
j. Change Management Program
k. Procedures for monitoring use of information processing facilities
l. Policies, operational plans, and procedures for teleworking activities
m. Policy on the use of cryptographic controls
n. Network diagram

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

2.3.2. Key Personnel Interviews

After collecting and reviewing relevant documentation, the ISF interviews key personnel (users, administrators, and management) to identify undocumented practices and gain feedback. As part of the interview process, the ISF discusses the actual practices in use and throughout the other phases of the assessment, the ISF identifies procedures in use based on the technical results of the assessment. This information allows the ISF to identify procedural gaps and good practices that are not fully documented in the formal policies and procedures. Additionally, the ISF gauges the level of user awareness during the interviews to determine if users outside of the IT function have an appropriate level of understanding of GIS and their role in protecting sensitive data and other critical assets. The following key personnel responsible for establishing and applying the GIS policy must be interviewed at a minimum.

a. Person with overall responsibility for the gaming operation
b. Compliance officer
c. GIS officer or head of the GIS function
d. Operational staff
e. Software developers

2.3.3. Administrative Controls Assessment

The ISF performs testing and evaluations to assess the effectiveness and adequacy of these administrative measures in mitigating risks and ensuring compliance with security requirements. This assessment typically addresses the following topics:

a. Policies, Standards and Guidelines
b. Organizational Security
c. Operations Management
d. Patch and Management Update
e. Monitoring System Access and Use
f. Change Management procedures
g. Asset Classification and Control
h. Contingency Planning
i. GIS Incident Response

2.3.4. Technical Controls Assessment

The ISF performs testing and evaluations to assess the effectiveness and adequacy of these technical safeguards in mitigating risks and protecting sensitive data. This assessment typically addresses the following topics:

a. Infrastructure Design
b. Network Surveying
c. Gaming Technical Security (GTS)
d. Network and Communications Security
e. Logical Access Controls
f. Operating Systems (OS) Security
g. Malicious Software Controls
h. Database Design and Configuration
i. Cryptographic Controls
j. System Monitoring
k. Reporting and Logging
l. System Development Controls

2.3.5. Physical and Environmental Controls Assessment

The ISF performs testing and evaluations to assess the effectiveness and adequacy of these controls in safeguarding against physical threats, environmental hazards, and unauthorized access to sensitive areas. This assessment typically addresses the following topics:

a. Location and Facility Security
b. Perimeter Security
c. Access Controls
d. Equipment Security
e. Intrusion Detection
f. Alarm Systems
g. Surveillance Systems
h. Heating, Ventilation and Air Conditioning
i. Power Systems
j. Power and Communications Cabling
k. Fire Detection and Suppression
l. Emergency Response

2.3.6. Risk Assessment

The ISF performs a Risk Assessment to identify non-conformities to any applicable GIS Control, and any potential threats and vulnerabilities that may not be explicitly listed in the GLI-GSF but were observed during the audit and may constitute a risk. The ISF must use an appropriate scoring system for gaming security (e.g. CVSS, ISO/IEC 31010, etc.) for assigning levels of severity (minor or major) to non-conformities, vulnerabilities, and threats, allowing prioritization of responses and resources. The scoring system used by the ISF must be identified in the GIS Controls Audit report.

2.4. Audit Frequency

2.4.1. Initial Audit

The Gaming Enterprise must have a GIS Controls Audit performed by an ISF within ninety days of the Gaming Enterprise commencing gaming operations within that jurisdiction unless the Regulatory Body has advised otherwise. Any postponement of the GIS Controls Audit as requested by the Gaming Enterprise, along with an updated schedule, must be authorized by the Regulatory Body.

NOTE: It is recommended for Regulatory Bodies to allow flexibility for GIS Controls Audit schedules for multi-jurisdictional Gaming Enterprises to allow consolidation of audits for multiple jurisdictions to a common schedule.

2.4.2. Annual Audit

The Gaming Enterprise must, as a rule, have another GIS Controls Audit performed by an ISF within twelve months of the previous GIS Controls Audit unless the Regulatory Body has advised otherwise. Any postponement of the GIS Controls Audit as requested by the Gaming Enterprise, along with an updated schedule, must be authorized by the Regulatory Body.

NOTE: It is recommended for Regulatory Bodies to allow flexibility for GIS Controls Audit schedules for multi-jurisdictional Gaming Enterprises to allow consolidation of audits for multiple jurisdictions to a common schedule.

2.4.3. Additional Audits

The Gaming Enterprise must, as a rule, have additional GIS Controls Audits performed by an ISF after any critical changes within the GPE, such as infrastructure or application upgrades and modifications, or the installation of new Critical System Components. The determination of what constitutes a "critical change" is based on the Gaming Enterprise's Risk Assessment process, the specific configuration of the GPE, and the requirements of the Regulatory Body. However, any change that could affect the security of the GPE or allow access to sensitive data and/or Critical System Components may be deemed a "critical change" by the Gaming Enterprise.

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

2.5. Audit Reports

The results of a GIS Controls Audit identify for Gaming Enterprises those areas in the operations where improvement should be considered and recommend strategies for improving those areas. The GIS Controls Audit report must be submitted to the Regulatory Body no later than ninety days after the GIS Controls Audit has been completed unless the Regulatory Body has advised otherwise. The GIS Controls Audit report must include all the following:

a. Executive Summary:
   i. The Gaming Enterprise's name and contact information;
   ii. A brief overview of the Gaming Enterprise's business model, gaming activities offered, Service Providers utilized, location, number of employees, website, certifications, and a high-level description of the IT infrastructure (including data centers, cloud services, etc.)

b. GIS Controls Audit Details:
   i. The ISF's name, company affiliation, contact information, and qualifications and experience of the individuals who conducted the GIS Controls Audit;
   ii. The date(s) of the GIS Controls Audit, including the request date, the start date, the completion date, and the report date;

c. Scope of the GIS Controls Audit:
   i. A high-level overview of the work undertaken, specifying the environments (e.g., development, production) operating and the GIS Controls against which the GIS Controls Audit was conducted.
   ii. Identification of Critical System Components and assets reviewed, detailing how these components and assets were selected as part of the GIS Controls Audit.
   iii. Specific tools and techniques used during the GIS Controls Audit, including software names, versions, and official websites for the tools employed.

d. Methodology:
   i. A detailed description of the audit approach, including enquiry based questions, observation, evidence, key persons interviewed
   ii. Any limitations or exclusions in the GIS Controls Audit, with justifications (e.g., certain systems were out of scope due to business requirements).

e. Evidence Collected:
   i. Documentation reviewed, including the names, dates, and versions.
   ii. Personnel interviewed, with roles, locations, names, dates, and versions of interviews.
   iii. Evidence (e.g., screenshots, logs) that clearly illustrates the non-conformities identified, including commands and tools used to discover these issues.
   iv. Sampling techniques used to verify the security posture, including the size and nature of the sample.

f. Findings and Results:
   i. A summary of the non-conformities discovered, categorized by severity (e.g., minor, major).
   ii. A detailed explanation of each non-conformity, supported by evidence (e.g., screenshots, logs).
   iii. An audit of the potential impact or risk associated with each identified non-conformity, considering the Gaming Enterprise's specific environment.
   iv. Recommended remediation steps for each identified non-conformity, with priority levels and suggested timelines for mitigation.
   v. The Gaming Enterprise's response to the findings and results, including the recommended remediation steps.

2.6. Remediation

If the ISF's GIS 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.

a. Each non-conformity must be addressed through the Gaming Enterprise's remediation process, including:
   i. Actions taken to determine the extent of and contain the specific non-conformity.
   ii. Root cause investigation to determine the most basic causes of the non-conformity.
   iii. Actions taken to correct the non-conformity and, in response to the root cause, to eliminate recurrence of the non-conformity.

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

b. Remediation steps to address each identified major non-conformity must be carried out immediately and the Regulatory Body and the ISF, if required by the Regulatory Body, must be notified of the actions taken within thirty days, unless otherwise specified by the Regulatory Body. If required by the Regulatory Body, the ISF must perform a follow up audit within a reasonable timeframe specified within the remediation plan to confirm the actions taken, evaluate their effectiveness, and determine whether the non-conformities have been resolved.
c. Remediation steps to address each identified minor non-conformity must be documented and sent by the Gaming Enterprise to the Regulatory Body and the ISF, if required by the Regulatory Body, for review within thirty days, unless otherwise specified by the Regulatory Body. If the actions are deemed satisfactory, they must be followed up at the next scheduled audit.
d. Once remediation steps have been taken, the Gaming Enterprise must provide the Regulatory Body and the ISF, if required by the Regulatory Body, with documentation evidencing completion.
e. The Gaming Enterprise must maintain remediation records, including objective evidence, for at least five years, unless otherwise specified by the Regulatory Body.

2.7. Independent Security Firm (ISF)

The GIS 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:

a. Have relevant education background or in other ways provide relevant qualifications in assessing GPEs;
b. Obtain and maintain certifications sufficient to demonstrate proficiency and expertise as a qualified security professional by recognized certification boards, either nationally or internationally. The following certifications may demonstrate suitability to complete the GIS Controls Audit:
    i. ISO/IEC 27001 Lead Auditor;
    ii. Certified Information Systems Auditor (CISA);
    iii. Certified Information Security Manager (CISM);
    iv. Certified Information Systems Security Professional (CISSP);
c. Have at least five years' experience performing information security audits within the gaming industry or, where acceptable to the Regulatory Body, other relevant experience auditing the security controls of a similar industry; and
d. Meet any other qualifications as prescribed by the Regulatory Body.

NOTE: Nothing herein is intended to prohibit the Regulatory Body's qualified staff from acting as an ISF, provided they are independent from the Gaming Enterprise being audited.

3. ALTERNATE GIS CONTROLS AND EXCEPTIONS

3.1. Alternate GIS Controls

It is recognized that GIS Controls applicable to a Gaming Enterprise may vary depending on their size, ownership structure, scope and complexity of operations, corporate strategy and risk profile. The Regulatory Body may, in its discretion, approve the implementation of alternate GIS Controls in lieu of those listed in the Appendix upon request by the Gaming Enterprise.

a. For each enumerated GIS Control for which the Gaming Enterprise wishes to use an alternate GIS Control, the Gaming Enterprise must demonstrate how the alternate GIS Control:
    i. Protects the integrity of gaming offered by the Gaming Enterprise;
    ii. Safeguards the critical assets used in connection with the GPE; and
    iii. Achieves a level of security and integrity sufficient to accomplish the purpose of the GIS Control it is to replace.
b. A Gaming Enterprise may only implement an alternate GIS Control upon Regulatory Body approval.
c. Proof of the Regulatory Body's approval of the alternate GIS Control must be provided to the ISF and be evaluated as a part of the annual GIS Controls Audit.

NOTE: It is the Regulatory Body's responsibility to determine when it is acceptable or permitted for a Gaming Enterprise to use alternate GIS Controls.

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

3.2. Small Gaming Enterprises

The Regulatory Body may, in its discretion, permit a small Gaming Enterprise to be exempt from compliance with the GIS Controls listed in the Appendix provided that:

a. The annual gross gaming revenue of the small Gaming Enterprise does not exceed a threshold set by the Regulatory Body; and
b. The small Gaming Enterprise implements alternate GIS Controls which meet the requirements of the previous section.

NOTE: Nothing herein is intended to prohibit the Regulatory Body from using alternate or additional criteria to define a small Gaming Enterprise.

3.3. Charitable Gaming Enterprises

The Regulatory Body may, in its discretion, permit a charitable Gaming Enterprise to be exempt from compliance with the GIS Controls listed in the Appendix provided that:

a. All proceeds are for the benefit of a charitable organization;
b. The charitable Gaming Enterprise is operated wholly by the charitable organization's employees or volunteers, and not by independent operators for the benefit of a charitable organization;
c. The annual gross gaming revenue of the charitable Gaming Enterprise does not exceed a threshold set by the Regulatory Body; and
d. The charitable Gaming Enterprise implements alternate GIS Controls which meet the requirements of the previous section.

NOTE: Nothing herein is intended to prohibit the Regulatory Body from using alternate or additional criteria to define a charitable Gaming Enterprise.

3.4. ISF Exceptions

The Regulatory Body may, in its discretion, permit a small Gaming Enterprise or charitable Gaming Enterprise to use an internal audit function or qualified employee within the Gaming Enterprise or parent company of the Gaming Enterprise, which is independent of the Gaming Enterprise as an ISF, for their GIS Controls Audits.

NOTE: It is the Regulatory Body's responsibility to determine when it is acceptable or permitted for a small Gaming Enterprise or charitable Gaming Enterprise to perform the GIS Controls Audit under these circumstances.

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

APPENDIX: GAMING INFORMATION SECURITY (GIS) CONTROLS

The Gaming Information Security (GIS) Controls, as specified in this Appendix, indicate which Gaming Implementation Group (GIG) the GIS Control applies to. To assist Gaming Enterprises of every size, GIGs are divided into three groups, based on the risk profile and resources a Gaming Enterprise has available to them to implement the GLI-GSF. Each GIG identifies a set of the GIS Controls that they need to implement. GIG2 builds upon GIG1, and GIG3 is comprised of all the GIS Controls.

GIG	Gaming Implementation Group (GIG) Description
GIG1	The GLI-GSF defines Implementation Group 1 (GIG1) as essential gaming security hygiene and represents an emerging minimum standard of GIS for all Gaming Enterprises. The GIS Controls included in GIG1 are what every Gaming Enterprise should apply to defend against the most common attacks. A GIG1 Gaming Enterprise typically has limited security expertise to dedicate towards protecting critical assets and personnel. A common concern of Gaming Enterprises is to keep their gaming operations operational, as they have a limited tolerance for downtime. The criticality of the sensitive data that they are trying to protect is low and principally surrounds employee and financial information. GIS Controls selected for GIG1 should be implementable with limited gaming security expertise and aimed to thwart general, non-targeted attacks. These GIS Controls will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.
GIG2	The GIS Controls selected for GIG2 can help security teams cope with increased operational complexity. Some GIS Controls will depend on Gaming Enterprise-grade technology and specialized expertise to properly install and configure. A GIG2 Gaming Enterprise employs individuals who are responsible for managing and protecting GPE infrastructure. These Gaming Enterprises typically support multiple departments with differing risk profiles based on job function and mission. Small Gaming Enterprise units may have regulatory compliance burdens. GIG2 Gaming Enterprises often store and process sensitive data and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. All Gaming Enterprises running land-based gaming operations in which the GPE is continuously communicating over internet/public networks (e.g. lotteries, casinos with off-site systems, retail sports wagering, etc.) are to be treated as GIG2 Gaming Enterprises, unless otherwise specified by the Regulatory Body.
GIG3	A GIG3 Gaming Enterprise commonly employs gaming security experts that specialize in the different facets of gaming security (e.g., risk management, penetration testing, application security). A GIG3 Gaming Enterprise's critical assets contain sensitive data or functions that are subject to regulatory and compliance oversight. A GIG3 Gaming Enterprise must address the availability of services and the integrity and confidentiality of sensitive data. Successful attacks can cause significant harm to Personally Identifiable Information (PII). GIS Controls selected for GIG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks. All Gaming Enterprises running online gaming operations (e.g. interactive gaming, online event wagering, etc.) are to be treated as GIG3 Gaming Enterprises, unless otherwise specified by the Regulatory Body.

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

A. Adopted CIS Critical Security Controls

To establish a clear and reasonable baseline for GIS Controls, the GLI-GSF incorporates by reference the following controls of the Center for Internet Security (CIS) Critical Security Controls, Version 8.1, which must be met by each Gaming Enterprise (Enterprise). The right side column indicates the applicable Gaming Implementation Group (GIG) the CIS Control applies to.

NOTE: The entire CIS Critical Security Controls Document is available free of charge at www.cisecurity.org.

CIS-1	Inventory and Control of Enterprise Assets	GIG
CIS-1.1	Establish and Maintain Detailed Enterprise Asset Inventory	GIG1
CIS-1.2	Address Unauthorized Assets	GIG1
CIS-2	Inventory and Control of Software Assets	GIG
CIS-2.1	Establish and Maintain a Software Inventory	GIG1
CIS-2.2	Ensure Authorized Software is Currently Supported	GIG1
CIS-2.3	Address Unauthorized Software	GIG1
CIS-3	Data Protection	GIG
CIS-3.1	Establish and Maintain a Data Management Process	GIG1
CIS-3.2	Establish and Maintain a Data Inventory	GIG1
CIS-3.4	Enforce Data Retention	GIG1
CIS-3.5	Securely Dispose of Data	GIG1
CIS-3.6	Encrypt Data on End-User Devices	GIG1
CIS-3.7	Establish and Maintain a Data Classification Scheme	GIG2
CIS-3.9	Encrypt Data on Removable Media	GIG2
CIS-3.10	Encrypt Sensitive Data in Transit	GIG2
CIS-3.11	Encrypt Sensitive Data at Rest	GIG2
CIS-3.14	Log Sensitive Data Access	GIG3
CIS-4	Secure Configuration of Enterprise Assets and Software	GIG
CIS-4.1	Establish and Maintain a Secure Configuration Process	GIG1
CIS-4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	GIG1
CIS-4.3	Configure Automatic Session Locking on Enterprise Assets	GIG1
CIS-4.4	Implement and Manage a Firewall on Servers	GIG1
CIS-4.6	Securely Manage Enterprise Assets and Software	GIG1
CIS-4.7	Manage Default Accounts on Enterprise Assets and Software	GIG1
CIS-4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	GIG2
CIS-4.9	Configure Trusted DNS Servers on Enterprise Assets	GIG2
CIS-4.10	Enforce Automatic Device Lockout on Portable End-User Devices	GIG2
CIS-5	Account Management	GIG
CIS-5.1	Establish and Maintain an Inventory of Accounts	GIG1
CIS-5.2	Use Unique Passwords	GIG1
CIS-5.3	Disable Dormant Accounts	GIG1
CIS-5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	GIG1
CIS-5.5	Establish and Maintain an Inventory of Service Accounts	GIG2
CIS-5.6	Centralize Account Management	GIG2

CIS-6	Access Control Management	GIG
CIS-6.1	Establish an Access Granting Process	GIG1
CIS-6.2	Establish an Access Revoking Process	GIG1
CIS-6.3	Require MFA for Externally-Exposed Applications	GIG1
CIS-6.4	Require MFA for Remote Network Access	GIG1
CIS-6.5	Require MFA for Administrative Access	GIG1
CIS-6.7	Centralize Access Control	GIG2
CIS-6.8	Define and Maintain Role-Based Access Control	GIG3
CIS-7	Continuous Vulnerability Management	GIG
CIS-7.1	Establish and Maintain a Vulnerability Management Process	GIG1
CIS-7.2	Establish and Maintain a Remediation Process	GIG1
CIS-7.3	Perform Automated Operating System Patch Management	GIG1
CIS-7.4	Perform Automated Application Patch Management	GIG1
CIS-7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	GIG2
CIS-7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	GIG2
CIS-7.7	Remediate Detected Vulnerabilities	GIG2
CIS-8	Audit Log Management	GIG
CIS-8.1	Establish and Maintain an Audit Log Management Process	GIG1
CIS-8.2	Collect Audit Logs	GIG1
CIS-8.3	Ensure Adequate Audit Log Storage	GIG1
CIS-8.4	Standardize Time Synchronization	GIG2
CIS-8.5	Collect Detailed Audit Logs	GIG2
CIS-8.9	Centralize Audit Logs	GIG2
CIS-8.11	Conduct Audit Log Reviews	GIG2
CIS-8.12	Collect Service Provider Logs	GIG3
CIS-9	Email and Web Browser Protections	GIG
CIS-9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	GIG1
CIS-9.2	Use DNS Filtering Services	GIG1
CIS-9.7	Deploy and Maintain Email Server Anti-Malware Protections	GIG3
CIS-10	Malware Defenses	GIG
CIS-10.1	Deploy and Maintain Anti-Malware Software	GIG1
CIS-10.2	Configure Automatic Anti-Malware Signature Updates	GIG1
CIS-10.6	Centrally Manage Anti-Malware Software	GIG2
CIS-10.7	Use Behavior-Based Anti-Malware Software	GIG2
CIS-11	Data Recovery	GIG
CIS-11.1	Establish and Maintain a Data Recovery Process	GIG1
CIS-11.2	Perform Automated Backups	GIG1
CIS-11.3	Protect Recovery Data	GIG1
CIS-11.4	Establish and Maintain an Isolated Instance of Recovery Data	GIG1
CIS-11.5	Test Data Recovery	GIG2

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

CIS-12	Network Infrastructure Management	GIG
CIS-12.1	Ensure Network Infrastructure is Up-to-Date	GIG1
CIS-12.2	Establish and Maintain a Secure Network Architecture	GIG2
CIS-12.3	Securely Manage Network Infrastructure	GIG2
CIS-12.4	Establish and Maintain Architecture Diagram(s)	GIG2
CIS-12.6	Use of Secure Network Management and Communication Protocols	GIG2
CIS-13	Network Monitoring and Defense	GIG
CIS-13.1	Centralize Security Event Alerting	GIG2
CIS-13.2	Deploy a Host-Based Intrusion Detection Solution	GIG2
CIS-13.3	Deploy a Network Intrusion Detection Solution	GIG2
CIS-13.4	Perform Traffic Filtering Between Network Segments	GIG2
CIS-13.7	Deploy a Host-Based Intrusion Prevention Solution	GIG3
CIS-13.8	Deploy a Network Intrusion Prevention Solution	GIG3
CIS-13.9	Deploy Port-Level Access Control	GIG3
CIS-13.10	Perform Application Layer Filtering	GIG3
CIS-14	Security Awareness and Skills Training	GIG
CIS-14.1	Establish and Maintain a Security Awareness Program	GIG1
CIS-14.2	Train Workforce Members to Recognize Social Engineering Attacks	GIG1
CIS-14.3	Train Workforce Members on Authentication Best Practices	GIG1
CIS-14.4	Train Workforce on Data Handling Best Practices	GIG1
CIS-14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	GIG1
CIS-14.9	Conduct Role-Specific Security Awareness and Skills Training	GIG2
CIS-15	Service Provider Management	GIG
CIS-15.1	Establish and Maintain an Inventory of Service Providers	GIG1
CIS-15.2	Establish and Maintain a Service Provider Management Policy	GIG2
CIS-15.3	Classify Service Providers	GIG2
CIS-15.4	Ensure Service Provider Contracts Include Security Requirements	GIG2
CIS-15.5	Assess Service Providers	GIG3
CIS-15.6	Monitor Service Providers	GIG3
CIS-15.7	Securely Decommission Service Providers	GIG3
CIS-16	Application Software Security	GIG
CIS-16.1	Establish and Maintain a Secure Application Development Process	GIG2
CIS-16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	GIG2
CIS-16.3	Perform Root Cause Analysis on Security Vulnerabilities	GIG2
CIS-16.4	Establish and Manage an Inventory of Third-Party Software Components	GIG2
CIS-16.5	Use Up-to-Date and Trusted Third-Party Software Components	GIG2
CIS-16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	GIG2
CIS-16.8	Separate Production and Non-Production Systems	GIG2
CIS-16.9	Train Developers in Application Security Concepts and Secure Coding	GIG2
CIS-16.12	Implement Code-Level Security Checks	GIG2
CIS-16.13	Conduct Application Penetration Testing	GIG3

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

CIS-17	Incident Response Management	GIG
CIS-17.1	Designate Personnel to Manage Incident Handling	GIG1
CIS-17.2	Establish and Maintain Contact Information for Reporting Security Incidents	GIG1
CIS-17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	GIG1
CIS-17.4	Establish and Maintain an Incident Response Process	GIG2
CIS-17.5	Assign Key Roles and Responsibilities	GIG2
CIS-17.6	Define Mechanisms for Communicating During Incident Response	GIG2
CIS-17.7	Conduct Routine Incident Response Exercises	GIG2
CIS-17.8	Conduct Post-Incident Reviews	GIG2
CIS-17.9	Establish and Maintain Security Incident Thresholds	GIG3
CIS-18	**Penetration Testing**	**GIG**
CIS-18.1	Establish and Maintain a Penetration Testing Program	GIG2
CIS-18.2	Perform Periodic External Penetration Tests	GIG2
CIS-18.3	Remediate Penetration Test Findings	GIG2
CIS-18.4	Validate Security Measures	GIG3
CIS-18.5	Perform Periodic Internal Penetration Tests	GIG3

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

B. Additional Common GIS Controls

In addition to the CIS Critical Security Controls adopted previously, the following additional GIS Controls apply to GPEs used for all forms of gaming. The right side column indicates the applicable Gaming Implementation Group (GIG) the GIS Control applies to.

GIS-1	GPE Critical Control Program Functions	GIG
GIS-1.1	**GPE Internal Clock**	
GIS-1.1.1	The GPE must maintain an internal clock that reflects the current date and time which must be used to provide for the time stamping of all transactions, configuration changes, and significant events, and as a reference clock for reporting using the Network Time Protocol (NTP) or equivalent.	**GIG1**
GIS-1.1.2	Changes to the internal clock's date and time, or the approved time sources, must be recorded in an audit log, indicating: a. The date and time of the changes; b. Reason and description of the changes, including initial and final values; and c. User account ID(s) who performed and/or authorized the changes.	**GIG1**
GIS-1.2	**Critical Control Program Signature Verification**	
GIS-1.2.1	Critical Control Programs must be identified and documented in order for the Gaming Enterprise to verify the integrity of the GPE.	**GIG1**
GIS-1.2.2	Each Critical Control Program must be verified as identical to those approved by the Regulatory Body via a signature verification procedure, which must be performed: a. Upon installation/updates of components; b. Upon power up or recovery from a shutdown state; c. At least once every 24 hours; and d. On demand.	**GIG1**
GIS-1.2.3	The signature verification procedure must: a. Operate independently of any process or security software within the system. b. Employ a cryptographic hash algorithm which produces a message digest of at least 128 bits. Other test methodologies must be reviewed on a case-by-case basis. c. Include one or more analytical steps to compare the current signatures of the Critical Control Programs in the GPE with the signatures of the current approved versions of the Critical Control Programs.	**GIG1**
GIS-1.2.4	The output of the signature verification procedure must be recorded in an audit log, detailing for each verification: a. The date and time of the verification; b. Identification of each verified Critical Control Program; c. The expected and generated signature results, including indication of any program error or signature mismatch; and d. When performed on demand, user account ID who initiated the verification procedure.	**GIG1**
GIS-1.2.5	Any failure of signature verification of any Critical Control Program must require a notification of the verification failure being communicated to the Gaming Enterprise and Regulatory Body as required.	**GIG1**
GIS-1.2.6	There must be a process in place for responding to signature verification failures, including determining the cause of the failure and performing the associated corrections or reinstallations of the Critical Control Program needed in a timely manner.	**GIG1**
GIS-2	**Gaming Information Security (GIS)**	**GIG**
GIS-2.1	**GIS Policy**	
GIS-2.1.1	A GIS policy must be defined and implemented to describe the Gaming Enterprise's approach to managing GIS and its implementation and to ensure that risks are identified, mitigated, and underwritten by contingency plans.	**GIG1**
GIS-2.1.2	The GIS policy must have a provision requiring review at least annually or at planned intervals required by the Regulatory Body and when significant changes occur to the GPE or the Gaming Enterprise's processes which alter the risk profile of the system.	**GIG1**
GIS-2.1.3	The GIS policy must be approved by management and communicated to and acknowledged by relevant personnel within the Gaming Enterprise.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-2.1.4	The GIS policy must delineate the security roles and responsibilities of relevant personnel within the Gaming Enterprise for the operation, service, and maintenance of the GPE. Some of these security roles and responsibilities may be assigned based on Risk Assessments performed by the Gaming Enterprise.	**GIG1**
GIS-2.2	**Access Control Policy**	
GIS-2.2.1	An access control policy must be established and documented based on business and security requirements for physical and logical access to the GPE, including remote access.	**GIG1**
GIS-2.2.2	The access control policy must be reviewed at least annually or as required by the Gaming Enterprise and/or the Regulatory Body.	**GIG1**
GIS-2.2.3	A formal user registration and de-registration procedure must be in place for granting and revoking access to the GPE.	**GIG1**
GIS-2.2.4	The allocation and use of user access rights and privileges must be restricted and controlled based on business requirements and the principle of least privilege.	**GIG2**
GIS-2.2.5	Personnel must only be provided with access to the services or facilities that they have been specifically authorized to use.	**GIG1**
GIS-2.2.6	Management must use a formal process to review and confirm user access rights and privileges at least annually or as required by the Gaming Enterprise and/or the Regulatory Body .	**GIG2**
GIS-2.3	**Allocation of GIS Responsibilities**	
GIS-2.3.1	GIS responsibilities must be effectively documented and implemented.	**GIG2**
GIS-2.3.2	A GIS forum comprised of management must be formally established to monitor and review the GIS policy to ensure its continuing suitability, adequacy, and effectiveness, maintain formal minutes of meetings, and convene at least every six months or at regular intervals required by the Regulatory Body.	**GIG2**
GIS-2.3.3	A GIS function must exist that will be responsible for developing and implementing security strategies and action plans in accordance with the overall Gaming Enterprise.	**GIG2**
GIS-2.3.4	The GIS function must be involved in reviewing all necessary tasks and processes regarding GIS aspects of the Gaming Enterprise, including, but not be limited to, the protection of information and sensitive data, communications, virtual and physical infrastructure, personnel, and overall operational security.	**GIG2**
GIS-2.3.5	The GIS function must report to executive level management with regard to the management of security risk.	**GIG2**
GIS-2.3.6	To avoid a conflict of interest between operations and security risk management The GIS function must be independent of the IT function unless otherwise authorized by the Regulatory Body.	**GIG2**
GIS-2.3.7	The GIS function must have the competences and be sufficiently empowered and must have access to all necessary resources to enable adequate assessment, management, and reduction of risk.	**GIG2**
GIS-2.3.8	The head of the GIS function must be a member of the GIS forum and be responsible for recommending GIS policies and changes.	**GIG2**
GIS-2.4	**Personally Identifiable Information (PII) Privacy Program**	
GIS-2.4.1	The Gaming Enterprise must establish and maintain a privacy program to provide adequate technical and organizational protections for PII collected or processed by the Gaming Enterprise.	**GIG1**
GIS-2.4.2	The privacy program must consider the overall fairness and transparency of how the Gaming Enterprise processes PII of individuals and protects such information in compliance with any local privacy regulations and standards observed by the Regulatory Body.	**GIG1**
GIS-2.4.3	The Gaming Enterprise must designate one or more individuals with primary responsibility for the design, implementation, and ongoing evaluation of procedures and practices related to the security and processing of PII.	**GIG1**
GIS-2.4.4	The Gaming Enterprise must establish procedures to determine the nature and scope of all PII collected and processed by the Gaming Enterprise, including the types of information collected and processed, sources of collection, and purposes of use.	**GIG1**
GIS-2.4.5	The Gaming Enterprise must adhere to and make publicly available a privacy notice to inform individuals of the PII processing activities of the Gaming Enterprise, including without limitation, a. Information pertaining to the purpose of the PII collection; b. Whether the PII will be shared or sold to other entities; and c. The manner for exercising individual rights, if applicable.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-2.4.6	If a Gaming Enterprise utilizes automated decision-making, the Gaming Enterprise must establish procedures for the governance of such process to ensure the legal rights of the individual are not infringed.	**GIG1**
GIS-2.5	**Securing Financial Transactions within the GPE**	
GIS-2.5.1	Payment methods used for financial transactions in the GPE must be protected from fraudulent use.	**GIG1**
GIS-2.5.2	The Gaming Enterprise must only collect the sensitive data strictly needed for the financial transaction.	**GIG1**
GIS-2.5.3	There must be processes in place for verifying the protection of sensitive data directly related to each financial transaction within the GPE, including any PII given by the patron or payment related data.	**GIG1**
GIS-2.5.4	Any communication channels within the GPE conveying financial transaction details must employ encryption to protect against interception.	**GIG1**
GIS-3	**GPE Operation & Security**	**GIG**
GIS-3.1	**Security Procedures**	
GIS-3.1.1	The Gaming Enterprise must monitor the Critical System Components and the transmission of data of the entire GPE, including communication, data packets, networks, applications, as well as the components and data transmissions of any Service Provider services involved, with the objective of ensuring integrity, reliability, and accessibility, as well as to identify anomalous behavior.	**GIG2**
GIS-3.1.2	The Gaming Enterprise must monitor and adjust GPE resource capacity and consumption to ensure availability is maintained.	**GIG1**
GIS-3.1.3	The Gaming Enterprise must maintain an audit log of the GPE performance, including a function to compile performance reports.	**GIG2**
GIS-3.1.4	The Gaming Enterprise must monitor its GPE in order to detect, prevent, mitigate, and respond to common active and passive technical attacks and compromises.	**GIG1**
GIS-3.1.5	The Gaming Enterprise must establish procedures to gather and analyze threat intelligence, and to act on it appropriately.	**GIG2**
GIS-3.1.6	The Gaming Enterprise must establish procedures to centrally monitor, manage, and respond to user activities, exceptions, malfunctions, and adverse events.	**GIG2**
GIS-3.2	**GPE Malfunctions**	
GIS-3.2.1	Upon detection of a malfunction, the Gaming Enterprise must initiate an investigation to determine the root cause of the malfunction.	**GIG1**
GIS-3.2.2	The investigation must involve a thorough review of relevant records, reports, audit logs, and surveillance records associated with the affected Critical System Component.	**GIG1**
GIS-3.2.3	Based on the documented findings of the investigation, appropriate actions must be taken to repair or replace the Critical System Components responsible for the malfunction.	**GIG1**
GIS-3.2.4	Prior to restoring the Critical System Components to operation, verification activities must be conducted to ensure its integrity and functionality.	**GIG1**
GIS-3.2.5	In accordance with regulatory requirements, the Gaming Enterprise must file a malfunction report with the appropriate Regulatory Body documenting the details of the malfunction.	**GIG1**
GIS-3.3	**GIS Incident Management**	
GIS-3.3.1	The Gaming Enterprise must define, monitor, and document, as well as report, investigate, respond to, and resolve GIS incidents, including detected breaches and suspected or actual hacking or tampering with the GPE.	**GIG1**
GIS-3.3.2	All GIS incidents must be responded to within an established time period approved by the Regulatory Body and formally documented.	**GIG1**
GIS-3.3.3	In the event of a GIS incident that compromises the security or integrity of sensitive data: a. The affected individuals, the Regulatory Body, and other relevant authorities must be promptly notified of the breach. b. The breach must be promptly reported to the Regulatory Body and other relevant authorities, including details about the nature of the GIS incident, potential risks, and steps taken to mitigate the impact.	**GIG1**
GIS-3.3.4	The GIS incident response plan must include documented procedures to handle various types of GIS incidents.	**GIG1**
GIS-3.3.5	Procedures must be established for the controlled recovery from GIS incidents, including restoring affected systems and sensitive data to a known good state.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-3.4	**Physical Location of Servers**	
GIS-3.4.1	The GPE servers, sensitive data, information, and other associated assets must be housed in one or more secure locations which may be located locally, within a single site or venue, or may be remotely located outside of the site or venue as allowed by the Regulatory Body.	**GIG1**
GIS-3.4.2	Each secure location must have sufficient protection against alteration, tampering or unauthorized access.	**GIG1**
GIS-3.4.3	Each secure location must be equipped with a surveillance system that must meet the procedures put in place by the Regulatory Body.	**GIG1**
GIS-3.4.4	Security measures for working in secure locations must be designed and implemented.	**GIG1**
GIS-3.4.5	Security perimeters must be defined and used to protect each secure location.	**GIG1**
GIS-3.4.6	Each secure location must be protected by appropriate entry controls to ensure that access is restricted to only authorized personnel.	**GIG1**
GIS-3.4.7	For physical access to each secure location, an auditable MFA process must be used unless the secure location is staffed at all times.	**GIG1**
GIS-3.4.8	Access devices to the secure location, such as magnetic swipe, proximity cards, embedded chip cards, fobs, keys, must be controlled by authorized personnel.	**GIG1**
GIS-3.4.9	All attempts at physical access to each secure location must be recorded in an audit log, indicating: a. The date and time the access attempt; b. Identification of the individual attempting access; c. Identification of the secure site or venue being accessed; d. Indication on whether or not the access attempt was successful; and e. If the access attempt was successful, the duration of the access.	**GIG1**
GIS-3.4.10	Each secure location must be equipped with controls to provide physical protection against damage from fire, flood, and other environmental threats and forms of natural or manmade disaster (e.g., hurricane, earthquake, etc.).	**GIG1**
GIS-3.4.11	The GPE must be protected from power surges, failures and other disruptions caused by failures in supporting utilities.	**GIG1**
GIS-3.4.12	Cables carrying power, data or supporting Critical System Components must be protected from interception, interference, or damage.	**GIG1**
GIS-3.4.13	All Critical System Components must be provided with adequate primary power.	**GIG1**
GIS-3.4.14	Where the server is a stand-alone application, it must have an Uninterruptible Power Supply (UPS) connected and must have sufficient capacity to permit a graceful shut-down and that retains all sensitive data during a power loss. It is acceptable that the system may be a component of a network that is supported by a network-wide UPS provided that the server is included as a device protected by the UPS. A surge protection system must be in use if not incorporated into the UPS itself.	**GIG1**
GIS-3.5	**Logical Access Control**	
GIS-3.5.1	The GPE must be logically secured against unauthorized access by authentication credentials allowed by the Regulatory Body, such as passwords, MFA, digital certificates, PINs, biometrics, and other access methods.	**GIG1**
GIS-3.5.2	Each user account must have their own individual authentication credential whose provision must be controlled through a formal process.	**GIG1**
GIS-3.5.3	Users must only have access to the functionality and features appropriate for their role and responsibilities within the system.	**GIG1**
GIS-3.5.4	It must not be possible to modify the critical system parameters of the GPE, including the policies and parameters for operating systems, databases, networks, and applications (e.g., audit settings, password complexity settings, system security levels, manual updates to databases, etc.), without an authorized secure process. Changes to critical system parameters must be recorded in an audit log, indicating: a. The date and time of the changes; b. Critical system parameters changed; c. Reason and description of the changes, including initial and final values; and d. User account ID(s) who performed and/or authorized the changes.	**GIG1**
GIS-3.5.5	The use of generic accounts must be limited, and where used the reasons for their use must be formally documented.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-3.5.6	Records for authentication credentials must be maintained either manually or by systems that automatically record authentication changes and force authentication credential changes.	**GIG1**
GIS-3.5.7	Any authentication credentials stored on the system must be either encrypted or hashed to other authorized cryptographic algorithms.	**GIG1**
GIS-3.5.8	A fallback method for resetting authentication credentials (e.g., forgotten passwords) must be at least as strong as the primary method. An MFA process must be employed for these purposes.	**GIG2**
GIS-3.5.9	Lost or compromised authentication credentials and authentication credentials of terminated users must be deactivated, secured, or destroyed as soon as reasonably possible.	**GIG1**
GIS-3.5.10	The system must have multiple security access levels to control and restrict different classes of access to the server, including viewing, changing, or deleting critical files and directories. Procedures must be in place to assign, review, modify, and remove access rights and privileges to each user, including: a. Allowing the administration of user accounts to provide an adequate separation of duties. b. Limiting the users who have the requisite permissions to adjust critical system parameters. c. The enforcement of adequate authentication credential parameters such as minimum length, and expiration intervals.	**GIG1**
GIS-3.5.11	A Service Provider within the Gaming Enterprise may, as needed, access the system and its associated components using a guest user account for product and user support or updates/upgrades, as permitted by the Regulatory Body and the Gaming Enterprise. The guest user accounts must be: a. Restricted through logical controls to access only the necessary application(s) and/or database(s) for the product and user support or providing updates/upgrades; b. Continuously monitored by the Gaming Enterprise; and c. Disabled when not in use and immediately after the purpose for which the account was established is no longer required.	**GIG1**
GIS-3.5.12	Procedures must be in place to identify and flag suspect user accounts to prevent their unauthorized use, which includes: a. Having system administrator notification and user lockout, after a maximum number of three incorrect attempts at authentication; b. Flagging of suspect accounts where authentication credentials may have been stolen; and c. Invalidating accounts and transferring critical stored account information into a new account.	**GIG1**
GIS-3.5.13	Any logical access attempts to the system applications or operating systems must be recorded in an audit log, indicating: a. The date and time the access attempt; b. User account ID; c. IP Address of the individual attempting access; d. Indication on whether or not the access attempt was successful; and e. If the access attempt was successful, the duration of the access.	**GIG1**
GIS-3.5.14	The use of utility programs which can override application or operating system controls must be restricted and tightly controlled.	**GIG1**
GIS-3.5.15	System voids, overrides, corrections, or any other activities requiring user intervention and occurring outside of the normal scope of system operation must be recorded in an audit log, indicating: a. The date and time of the activities; b. Components affected by the activities; c. Reason and description of the activities, including initial and final values; and d. User account ID(s) who performed and/or authorized the activities.	**GIG1**
GIS-3.5.16	For each user account, the information to be maintained and backed up by the GPE must include: a. User account ID; b. Individual name and title or position; c. Full list and description of functions that each group or user account may execute; d. The date and time the account was created; e. The date and time of last access, including IP Address; f. The date and time of last password change; g. The date and time the account was disabled/deactivated; h. Description of the access rights or group membership of the account, if applicable; and i. The current and previous statuses of the user account (e.g., active, inactive, closed, suspended, etc.).	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-3.5.17	Only authorized personnel may have access to inactive or closed user accounts.	**GIG1**
GIS-3.6	**User Authentication and Authorization**	
GIS-3.6.1	A secure and controlled mechanism must be employed that can verify that the Critical System Component is being accessed by authorized personnel on demand and on a regular basis as required by the Regulatory Body.	**GIG1**
GIS-3.6.2	Active sessions must be terminated if user authorization has exceeded a configurable number of failed attempts.	**GIG1**
GIS-3.6.3	When used, automated equipment identification methods to authenticate connections from specific locations and equipment must be documented and must be included in the review of access rights and privileges.	**GIG2**
GIS-3.6.4	Any authorization information communicated by the system for identification purposes must be obtained at the time of the request from the system and not be stored on the system component.	**GIG2**
GIS-3.6.5	Where user sessions are tracked for authorization, the user session authorization information must always be created randomly, in memory, and must be removed after the user's session has ended.	**GIG2**
GIS-3.6.6	Restrictions on connection times such as but not necessarily limited to session timeouts must be used to provide additional security for high-risk applications, such as remote access.	**GIG1**
GIS-3.7	**Server Programming**	
GIS-3.7.1	The GPE must be sufficiently secure to prevent any unauthorized user-initiated programming capabilities on the server that may result in modifications to the database. However, it is acceptable for network or system administrators to perform authorized network infrastructure maintenance or application troubleshooting with sufficient access rights.	**GIG1**
GIS-3.7.2	The server must also be protected from the unauthorized execution of mobile code. This includes preventing the execution of potentially harmful code that may be introduced through mobile devices or other external sources.	**GIG2**
GIS-3.8	**Cloud and Virtualized Environments**	
GIS-3.8.1	If sensitive data is stored, processed or transmitted in a cloud or virtualized environment, appropriate GIS Controls must apply to that environment. This typically involves validating both the infrastructure and the usage of server instances within the cloud or virtualization environment.	**GIG2**
GIS-3.8.2	Redundant server instances in a cloud or virtualized environment must not run under the same hypervisor.	**GIG2**
GIS-3.8.3	Each server instance in a cloud or virtualized environment may perform only one critical function.	**GIG3**
GIS-3.9	**Optional Use of an Electronic Document Retention System (ERDS)**	
GIS-3.9.1	The ERDS must be properly configured to maintain the original version along with all subsequent versions reflecting all changes to reports or audit logs that are stored in an alterable format.	**GIG1**
GIS-3.9.2	The ERDS must maintain a unique signature for each version of the audit log, including the original.	**GIG1**
GIS-3.9.3	The ERDS must retain an audit log of changes to all reports including the user account ID performed the changes, the date and time the changes occurred, and what was changed.	**GIG1**
GIS-3.9.4	The ERDS must provide a method of complete indexing for easily locating and identifying the audit log including at least the following (which may be input by the user): a. Date and time the audit log was generated; b. Critical system component generating the audit log; c. Title and description of the audit log; d. User account ID of who is generating the audit log; and e. Any other information that may be useful in identifying the audit log and its purpose.	**GIG1**
GIS-3.9.5	The ERDS must be configured to a. Limit access to modify or add reports or audit logs to the system through logical security of specific user accounts; and b. Provide an audit log of all administrative user account activity.	**GIG1**
GIS-3.9.6	The ERDS must be properly secured using physical and logical security measures (user accounts with appropriate access, proper levels of event logging, and document the version control, etc.).	**GIG1**
GIS-3.9.7	The ERDS must be equipped to prevent disruption of log availability and loss of data through hardware and software redundancy best practices, and backup processes.	**GIG1**

GIS-4	Data Integrity	GIG
GIS-4.1	**Sensitive Data Management**	
GIS-4.1.1	The Gaming Enterprise must provide a layered approach to GPE security to ensure secure storage and processing of sensitive data using reasonable protection methods.	**GIG1**
GIS-4.1.2	The Gaming Enterprise must implement a policy for maintaining sensitive data for at least five years, unless otherwise specified by the Regulatory Body, and in accordance with local data retention regulations and standards observed by the Regulatory Body.	**GIG1**
GIS-4.1.3	Appropriate methods for handling sensitive data must be implemented, including validation of input and rejection of corrupt sensitive data.	**GIG2**
GIS-4.1.4	Encryption or equivalent security must be used for files and directories containing sensitive data. If encryption is not used, the Gaming Enterprise must restrict users from viewing the contents of such files and directories, which at a minimum must provide for the segregation of system duties and responsibilities as well as the monitoring and recording of access by any person to such files and directories.	**GIG2**
GIS-4.1.5	Authorized alterations to the GPE's live data files and database tables occurring outside of normal program and operating system execution must be recorded in an audit log, indicating: a. The date and time of the alterations; b. The live data files and database tables affected by the alterations; c. Reason and description of the alterations, including live data files and database tables before and after the alterations; and d. User account ID(s) who performed and/or authorized the alteration.	**GIG1**
GIS-4.1.6	The GPE must provide a logical means for securing and protecting sensitive data against alteration, tampering, or unauthorized access, both external and internal.	**GIG1**
GIS-4.1.7	The normal operation of any Critical System Component that holds sensitive data must not have any options or mechanisms that may compromise the sensitive data.	**GIG1**
GIS-4.1.8	No Critical System Components may have a mechanism whereby an error will cause the sensitive data to automatically clear.	**GIG1**
GIS-4.1.9	Any Critical System Component that holds sensitive data in its memory must not allow removal of the information unless it has first transferred that information to the associated database or other secured component(s) of the system.	**GIG1**
GIS-4.1.10	The Gaming Enterprise must protect the confidentiality, integrity, accountability, and availability of sensitive data when held at-rest on servers, critical applications, and associated databases containing sensitive data, including limiting the number of workstations where they can be accessed.	**GIG2**
GIS-4.1.11	Encryption must be applied to protect the confidentiality, integrity, accountability, and availability of sensitive data when it's in use, when it's stored on portable computer systems (e.g. laptops, USB devices, etc.), and when it's held at-rest on workstations.	**GIG2**
GIS-4.1.12	Sensitive data that is not required to be hidden but must be authenticated must use some form of message authentication technique.	**GIG2**
GIS-4.1.13	Authentication must use a security certificate from an approved Gaming Enterprise, containing information about whom it belongs to, who it was issued by, valid dates, a unique serial number or other unique identification that can be used to verify the contents of the certificate.	**GIG1**
GIS-4.1.14	Production databases containing sensitive data must reside on networks separated from the servers hosting any patron interfaces.	**GIG1**
GIS-4.1.15	Sensitive data must be maintained at all times regardless of whether the server is being supplied with power.	**GIG1**
GIS-4.1.16	Sensitive data leakage prevention measures must be applied to systems, networks and any other devices that process, store, or transmit sensitive data.	**GIG2**
GIS-4.1.17	Sensitive data must be stored in such a way as to prevent the loss of the data when replacing parts or modules during normal maintenance.	**GIG1**
GIS-4.1.18	The alteration of any sensitive data must not be permitted without supervised access controls. In the event any sensitive data is changed, the following information must be documented or logged: a. The date and time of the alteration; b. Identification of the sensitive data altered; c. Reason and description of the sensitive data alteration, including initial and final values; and d. User account ID(s) who performed and/or authorized the alteration.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-4.1.19	Any irrecoverable loss of sensitive data must be recorded in an audit log, indicating; a. The date and time of the loss; b. Identification of the sensitive data lost; and c. Reason and description of the sensitive data lost.	**GIG1**
GIS-4.1.20	Sensitive data must be accessible by the Regulatory Body in a format which permits analysis by the Regulatory Body.	**GIG1**
GIS-4.2	**Backup Process Implementation**	
GIS-4.2.1	Backup process implementation must occur at least daily or as otherwise specified by the Regulatory Body, although all methods must be reviewed on a case-by-case basis.	**GIG1**
GIS-4.2.2	Sensitive data, critical applications, and associated databases must be backed up with immutability safeguards to prevent alterations or deletions, ensuring GPE integrity.	**GIG1**
GIS-4.2.3	Mirrored or redundant copies of sensitive data must be kept on the GPE with open support for backups and restoration.	**GIG1**
GIS-4.2.4	The backup must be contained on a non-volatile physical medium, or an equivalent architectural implementation.	**GIG1**
GIS-4.2.5	If HHDs are used as backup storage, data integrity must be assured in the event of a disk failure.	**GIG1**
GIS-4.2.6	Upon completion of the backup process, the backup storage is immediately transferred to a storage location physically separate from the location housing the servers and sensitive data being backed up (for temporary and permanent storage).	**GIG1**
GIS-4.2.7	The backup storage location must be secured to prevent unauthorized access and provides adequate protection to prevent the permanent loss of any sensitive data.	**GIG1**
GIS-4.2.8	If the backup is stored in a cloud platform, another copy may be stored in a different cloud platform or region.	**GIG2**
GIS-4.2.9	Backup data files and data recovery components must be managed with at least the same level of security and access controls as the GPE.	**GIG1**
GIS-4.2.10	In accordance with the agreed backup process, backup data files and data recovery components must be maintained, protected, and tested at least annually or as otherwise specified by the Regulatory Body.	**GIG2**
GIS-4.3	**System Failure and Recovery**	
GIS-4.3.1	The GPE must have sufficient redundancy and modularity so that if any single Critical System Component or part of a component fails, the functions of the GPE and the process of auditing those functions can continue with no loss or corruption of sensitive data.	**GIG1**
GIS-4.3.2	Significant periods of unavailability of any Critical System Component (any length of time operations is halted for all users, and/or transactions cannot be successfully completed for any user) must be recorded in an audit log, indicating; a. Identification of the unavailable component; b. The date and time the component became unavailable; and c. Reason and description of the component unavailability; d. The date and time the component became available again.	**GIG1**
GIS-4.3.3	When two or more Critical System Components are linked a procedure must be in place for the components to be tested after installation but prior to use in a GPE.	**GIG1**
GIS-4.3.4	The process of all gaming operations between the Critical System Components must not be adversely affected by restart or recovery of either component (e.g., transactions are not to be lost or duplicated because of recovery of one component or the other).	**GIG1**
GIS-4.3.5	Upon restart or recovery, the Critical System Components must immediately synchronize the status of all transactions, sensitive data, and configurations with one another.	**GIG1**
GIS-4.3.6	The Gaming Enterprise must be able to identify and properly handle the situation where a master reset has occurred on any Critical System Component.	**GIG1**
GIS-4.4	**Business Continuity and Disaster Recovery Plan**	
GIS-4.4.1	A business continuity and disaster recovery plan must be in place to recover gaming operations if the GPE is rendered inoperable, including, but not limited to: a. Data backup restoration; b. Program restoration; and c. Redundant or backup hardware restoration.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-4.4.2	The business continuity and disaster recovery plan must consider disasters including, but not limited to, those caused by weather, water, flood, fire, environmental spills and accidents, malicious destruction, acts of terrorism or war, and contingencies such as strikes, epidemics, pandemics, etc.	**GIG1**
GIS-4.4.3	The business continuity and disaster recovery plan must address the method of storing sensitive data to minimize loss. If asynchronous replication is used, the method for recovering information must be described or the potential loss of information must be documented.	**GIG2**
GIS-4.4.4	The business continuity and disaster recovery plan must delineate the circumstances under which it will be invoked.	**GIG1**
GIS-4.4.5	The business continuity and disaster recovery plan must address the establishment of a recovery site physically separated from the production site. The distance between the two locations should be determined based on potential environmental threats and hazards, power failures, and other disruptions but should also consider the potential difficulty of data replication as well as being able to access the recovery site within a reasonable time (Recovery Time Objective).	**GIG3**
GIS-4.4.6	The business continuity and disaster recovery plan must contain recovery guides detailing the technical steps required to re-establish gaming functionality at the recovery site.	**GIG1**
GIS-4.4.7	The business continuity and disaster recovery plan must address the processes required to resume administrative operations of gaming activities after the activation of the recovered system for a range of scenarios appropriate for the operational context of the system.	**GIG1**
GIS-4.4.8	The business continuity and disaster recovery plan must be tested at least annually or as otherwise specified by the Regulatory Body. The results of the testing must be documented.	**GIG1**
GIS-5	**Communications**	**GIG**
GIS-5.1	**Connectivity**	
GIS-5.1.1	Only authorized devices must be permitted to establish communications between any Critical System Components.	**GIG1**
GIS-5.1.2	The GPE must provide a method to a. Perform mutual authentication to ensure that authorized devices only communicate with valid networks; b. Enroll and un-enroll Critical System Components; and c. Enable and disable specific Critical System Components.	**GIG1**
GIS-5.1.3	Only enrolled and enabled Critical System Components may participate in gaming operations.	**GIG1**
GIS-5.1.4	The default condition for Critical System Components must be un-enrolled and disabled.	**GIG1**
GIS-5.1.5	The GPE must record the establishment, loss, and reestablishment of communications between Critical System Components in an audit log.	**GIG1**
GIS-5.2	**Communication Protocol**	
GIS-5.2.1	Each Critical System Component of the GPE must function as indicated by a documented secure communication protocol.	**GIG1**
GIS-5.2.2	All protocols must use communication techniques that have proper error detection and recovery mechanisms, which are designed to prevent intrusion, interference, eavesdropping, unauthorized alterations, and tampering. Any alternative implementations must be reviewed on a case-by-case basis and approved by the Regulatory Body.	**GIG1**
GIS-5.2.3	All critical communications of sensitive data must employ encryption and authentication for integrity.	**GIG1**
GIS-5.2.4	Communications on the secure network must only be possible between authorized Critical System Components that have been enrolled and authenticated as valid on the network. No unauthorized communications to components and/or access points must be allowed.	**GIG1**
GIS-5.2.5	Communications must be hardened to be immune to all possible malformed message attacks.	**GIG1**
GIS-5.2.6	Failure of communications must not affect the integrity of sensitive data.	**GIG1**
GIS-5.2.7	After a system interruption or shutdown, communication with all Critical System Components necessary for GPE operation must not be established and authenticated until the program resumption routine, including any self-tests, is completed successfully.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-5.3	**Communications Over Internet/Public Networks**	
GIS-5.3.1	Communications between any Critical System Components which takes place over internet/public networks, must be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification by encrypting the data packets or by utilizing a secure communications protocol to ensure the confidentiality and integrity of the transmission.	**GIG1**
GIS-5.3.2	Sensitive data must always be encrypted over the internet/public network and safeguarded from incomplete transmissions, misrouting, unauthorized message modification, disclosure, duplication, or replay.	**GIG1**
GIS-5.4	**Wireless Local Area Network (WLAN) Communications**	
GIS-5.4.1	Use of WLAN communications must be secured and only used where appropriate and not in areas where it could be potentially harmful.	**GIG1**
GIS-5.4.2	Communications between wireless devices on the WLAN must use protocols designed for securing, authenticating, and encrypting wireless networks.	**GIG1**
GIS-5.4.3	Multi-Factor Authentication (MFA) must be required at the wireless network and device level.	**GIG1**
GIS-5.4.4	Authentication schemes using Public Key Infrastructure (PKI) must require certificate validation, ideally in both directions (e.g. client certificates).	**GIG1**
GIS-5.4.5	Advanced Encryption Standards (AES) or equivalent with a minimum of 256-bit encryption must be used to support integrity and confidentiality services.	**GIG1**
GIS-5.4.6	The Pairwise Master Key (PMK) utilized must have a lifetime of twenty-four hours or less. Alternatively, it is acceptable for the PMK to be changed during pre-scheduled maintenance downtime in accordance with the GIS Controls adopted by the Gaming Enterprise.	**GIG1**
GIS-5.4.7	The Group Master Key (GMK) utilized must have a lifetime of eight hours or less.	**GIG1**
GIS-5.4.8	Wired Equivalent Privacy (WEP) must not be used. If it is not possible for the GPE to use the WPA2 protocol, the implementation of WEP as a secure encryption and authentication method must be reviewed on a case-by-case basis.	**GIG1**
GIS-5.4.9	One of the following encrypted tunneling protocols or equivalent must be utilized to secure communication of all sensitive data over the WLAN: a. Protected Extensible Authentication Protocol (Protected EAP or PEAP); b. Extensible Authentication Protocol - Transport Layer Security (EAP-TLS); c. Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS); d. Virtual Private Network (VPN) with L2TP/IPsec; e. Point to Point Tunneling Protocol (PPTP); or f. Secure Sockets Layer (SSL).	**GIG1**
GIS-5.4.10	The encrypted tunneling protocols must be authenticated against Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), Kerberos or Microsoft Active Directory servers or equivalent, as well as local databases stored on the secure gateway controller.	**GIG1**
GIS-5.5	**Wireless Access Points (WAP)**	
GIS-5.5.1	A WAP allows wireless devices to connect to a wired network using wireless transport (e.g. Wi-Fi) and relay data between the wireless device(s) and the rest of the network.	**GIG1**
GIS-5.5.2	The default administration login and password must be changed from the factory default to a secure value controlled according to the Gaming Enterprise.	**GIG1**
GIS-5.5.3	The default network password must be changed from the factory default to a secure value controlled according to the Gaming Enterprise.	**GIG1**
GIS-5.5.4	The SSID must be changed from the factory default to a secure value which does not contain any reference to the site name, manufacturer, or any other reference that could be easily discerned.	**GIG1**
GIS-5.5.5	Access to the administrative functions of the WAP must be restricted to connections from the wired side of the network utilizing a secure protocol with a privileged user account defined by the Gaming Enterprise.	**GIG1**
GIS-5.5.6	If the router supports WPA2 authentication, all WAPs must be IEEE 802.11 compliant and configured with Enterprise Mode enabled or with a strong pre-shared key.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-5.6	**Network Communication Equipment (NCE)**	
GIS-5.6.1	The Gaming Enterprise must provide a secure location for the placement, operation, and usage of NCE.	**GIG1**
GIS-5.6.2	NCE must be installed according to a defined plan and records of all installed NCE must be maintained.	**GIG1**
GIS-5.6.3	NCE must be constructed in such a way as to be resistant to physical damage to the hardware or corruption of the contained software by normal usage.	**GIG1**
GIS-5.6.4	NCE must be physically secured from unauthorized access.	**GIG1**
GIS-5.6.5	GPE communications via NCE must be logically secured from unauthorized access.	**GIG1**
GIS-5.6.6	NCE with limited onboard storage must, if the audit log becomes full, disable all communication or offload audit logs to a dedicated audit log server.	**GIG1**
GIS-5.7	**Intrusion Detection System/Intrusion Prevention System (IDS/IPS)**	
GIS-5.7.1	An IDS/IPS must be installed which includes one or more components that can listen to both internal and external communications as well as detect or prevent: a. Distributed Denial-of-Service (DDoS) attacks; b. Shellcode from traversing the network; c. Address Resolution Protocol (ARP) spoofing; and d. Other Man-In-The-Middle (MITM) attack indicators and sever communications immediately if detected.	**GIG1**
GIS-5.7.2	The IDS/IPS must scan the network for any unauthorized or rogue access points or devices connected to any access point on the network at least quarterly or as otherwise specified by the Regulatory Body.	**GIG2**
GIS-5.7.3	The IDS/IPS must automatically disable any unauthorized or rogue devices connected to the GPE.	**GIG2**
GIS-5.7.4	The IDS/IPS must maintain an audit log for access which must: a. Contain complete and comprehensive information about all devices involved, including the time and date, the name, and the hardware identifier of all devices requesting access to the network; and b. Be able to be reconciled with all other networking devices within the GPE.	**GIG1**
GIS-5.8	**Network Security Management**	
GIS-5.8.1	The Gaming Enterprise must review and update policies and procedures to ensure the network is secure and threats and vulnerabilities are addressed accordingly.	**GIG1**
GIS-5.8.2	Networks must be logically separated such that there should be no network traffic on a network link which cannot be serviced by hosts on that link.	**GIG1**
GIS-5.8.3	All network management functions must authenticate all users on the network and encrypt all network management communications.	**GIG1**
GIS-5.8.4	The failure of any single item must not result in a Denial-of-Service (DOS).	**GIG1**
GIS-5.8.5	All entry and exit points to the network must be identified, managed, controlled, and monitored on a 24/7 basis.	**GIG2**
GIS-5.8.6	All network hubs, services and connection ports must be secured to prevent unauthorized access to the network.	**GIG1**
GIS-5.8.7	Unused services and non-essential ports must be either physically blocked or software disabled whenever possible.	**GIG1**
GIS-5.8.8	Stateless protocols, such as User Datagram Protocol (UDP), must not be used for sensitive data without stateful transport. Note that although Hypertext Transport Protocol (HTTP) is technically stateless, if it runs on Transmission Control Protocol (TCP) which is stateful, this is allowed.	**GIG1**
GIS-5.8.9	All changes to network infrastructure must be recorded in an audit log, indicating: a. The date and time of the changes; b. Reason and description of the changes, including initial and final values; and c. User account ID(s) who performed and/or authorized the changes.	**GIG1**
GIS-5.9	**Telecommuting and Mobile Computing**	
GIS-5.9.1	Telecommuting must only be permitted under circumstances where the security of the endpoint can be assured .	**GIG1**
GIS-5.9.2	A formal policy must be in place, and supporting security measures must be adopted to protect against the risks of using mobile computing and communication facilities.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-6	Service Providers	GIG
GIS-6.1	**Service Provider Relationships**	
GIS-6.1.1	The allocation of responsibility between a Service Provider and the other entities within the Gaming Enterprise for managing GIS Controls does not exempt a Gaming Enterprise from the responsibility of ensuring that sensitive data is properly secured according to the applicable requirements.	**GIG1**
GIS-6.1.2	Where sensitive data is shared with Service Providers, formal data processing agreements must be in place that states the rights and obligations of each party concerning the protection of the sensitive data, including: a. The subject matter and duration of the processing; b. The nature and purpose of the processing; c. The type of data to be processed; d. How the data is stored; e. The detail of the security surrounding the data; f. The means used to transfer the data from one Gaming Enterprise to another; g. The means used to retrieve data about certain individuals; h. The method for ensuring a retention schedule is adhered to; i. The means used to delete or dispose of the data; and j. The categories of data.	**GIG1**
GIS-6.2	**Service Provider Communications**	
GIS-6.2.1	The GPE must be capable of securely communicating with Service Providers using encryption and strong authentication.	**GIG1**
GIS-6.2.2	All login events involving Service Providers must be recorded in an audit log.	**GIG1**
GIS-6.2.3	Communication with Service Providers must not interfere with or degrade normal GPE functions.	**GIG1**
GIS-6.2.4	Service Provider data must not affect patron communications.	**GIG1**
GIS-6.2.5	Service Providers must be on a segmented network separate from network segments hosting patron connections.	**GIG1**
GIS-6.2.6	Gaming must be disabled on all network connections except for those within the GPE.	**GIG1**
GIS-6.2.7	The GPE must not route data packets from Service Providers directly to the GPE and vice-versa.	**GIG1**
GIS-6.2.8	The GPE must not act as IP routers between the GPE and Service Providers.	**GIG1**
GIS-6.2.9	Unauthorized Service Providers must be prevented from viewing or altering sensitive data.	**GIG1**
GIS-7	**Technical Controls**	**GIG**
GIS-7.1	**Domain Name Service (DNS) Requirements**	
GIS-7.1.1	The Gaming Enterprise must utilize a secure primary DNS server and a secure secondary DNS server which are logically and physically separate from one another, enhancing resilience against single points of failure and potential attacks.	**GIG2**
GIS-7.1.2	The primary DNS server must be physically located in a secure data center or a virtualized host in an appropriately secured hypervisor or equivalent to prevent unauthorized access.	**GIG2**
GIS-7.1.3	Logical and physical access to the DNS servers must be restricted to authorized personnel through Multi-Factor Authentication (MFA), ensuring that only authenticated users can access the DNS servers and that DNS records are kept secure from malicious and unauthorized changes.	**GIG2**
GIS-7.1.4	Zone transfers to arbitrary hosts must be disallowed. This restriction prevents unauthorized parties from accessing or replicating DNS zone data, reducing the risk of data exposure or manipulation.	**GIG2**
GIS-7.1.5	A method to prevent cache poisoning, such as DNS Security Extensions (DNSSEC), is required.	**GIG2**
GIS-7.1.6	Registry lock must be in place, so any request to change DNS server(s) will need to be verified manually.	**GIG2**
GIS-7.2	**Cryptographic Controls**	
GIS-7.2.1	A policy on the use of cryptographic controls for the protection of sensitive data must be developed and implemented, ensuring that all cryptographic controls utilize cryptographic modules for secure execution and protection.	**GIG1**
GIS-7.2.2	The grade of encryption used must be appropriate to the sensitivity of the data.	**GIG1**
GIS-7.2.3	The use of encryption methods must be reviewed at least annually or as otherwise specified by the Regulatory Body to verify that the current encryption algorithms and key lengths are secure.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-7.2.4	The encryption method must include the use of different encryption keys so that encryption algorithms can be changed or replaced to correct weaknesses as soon as practical. Other methodologies must be reviewed on a case-by-case basis.	**GIG1**
GIS-7.2.5	The management of encryption keys throughout their whole lifecycle must follow defined processes established by the Gaming Enterprise.	**GIG1**
GIS-7.2.6	The Gaming Enterprise must establish procedures for obtaining or generating encryption keys, ensuring that only authorized personnel are involved in the process.	**GIG1**
GIS-7.2.7	Encryption keys must be stored on a secure and redundant storage medium after being encrypted themselves through a different encryption method and/or by using a different encryption key.	**GIG1**
GIS-7.2.8	Procedures must be established to monitor the expiration dates of encryption keys, where applicable.	**GIG1**
GIS-7.2.9	Procedures must be defined for promptly revoking encryption keys in the event of compromise, loss, or unauthorized access.	**GIG1**
GIS-7.2.10	Procedures must be established for securely changing the current encryption keyset, including the generation of new keys and the retirement of old keys.	**GIG1**
GIS-7.2.11	The Gaming Enterprise must implement procedures for recovering data secured with revoked or expired encryption keys for a defined period after the keys become invalid.	**GIG1**
GIS-7.3	**Critical System Component Hardening**	
GIS-7.3.1	Critical System Component configurations must be established, documented, implemented, monitored, and reviewed.	**GIG1**
GIS-7.3.2	Configuration procedures for Critical System Components must address all known security vulnerabilities and be consistent with industry-accepted best practices for system hardening.	**GIG1**
GIS-7.3.3	The appropriateness and effectiveness of steps taken to harden Critical System Components must be assessed at least annually or as otherwise specified by the Regulatory Body and, if appropriate, changes must be made to improve the hardening.	**GIG2**
GIS-7.3.4	All default or standard configuration parameters must be removed from all Critical System Components where a security risk is presented.	**GIG1**
GIS-7.3.5	Only one primary function must be implemented per server to prevent functions that require different security levels from co-existing on the same server.	**GIG1**
GIS-7.3.6	Additional security features must be implemented for any required services, protocols or daemons that are considered to be insecure.	**GIG1**
GIS-7.3.7	System security parameters must be configured to prevent misuse.	**GIG1**
GIS-7.3.8	All unnecessary functionalities must be removed, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**GIG1**
GIS-7.4	**Generation and Storage of Security Reports or Logs**	
GIS-7.4.1	Security reports or logs must be predefined and generated on each Critical System Component to monitor and rectify anomalies, flaws, and alerts.	**GIG1**
GIS-7.4.2	Security reports or logs must be protected against tampering and unauthorized access.	**GIG2**
GIS-7.4.3	Security reports or logs must be reviewed at least every ninety days or as otherwise specified by the Regulatory Body.	**GIG1**
GIS-8	**Remote Access and Firewalls**	**GIG**
GIS-8.1	**Remote Access Security**	
GIS-8.1.1	Remote access security must be reviewed on a case-by-case basis, in conjunction with the implementation of the current technology and approval from the Regulatory Body.	**GIG1**
GIS-8.1.2	Remote access methods must be appropriately secured and managed.	**GIG1**
GIS-8.1.3	The GPE must have the ability to enable or disable remote access, and the default state must be set to disabled	**GIG1**
GIS-8.1.4	Remote access must accept only the remote connections permissible by the firewall application and system settings.	**GIG1**
GIS-8.1.5	Remote access must be limited to only the application functions necessary for users to perform their job duties.	**GIG1**
GIS-8.1.6	No unauthorized remote user administration functionality (adding users, changing permissions, etc.) is permitted.	**GIG1**
GIS-8.1.7	Unauthorized remote access to the operating system or to any database other than information retrieval using existing functions is prohibited.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

GIS-8.1.8	The GPE must maintain an audit log depicting all remote access information and activity. Remote access logs must minimally include the following: a. User account ID(s) who performed and/or authorized the remote access, including verification of authorization; b. Remote IP Addresses, Port Numbers, Protocols, and where possible, MAC Addresses; c. Time and date the connection was made and duration of connection; d. Reason for remote access and description of work to be performed; e. Activity while logged in, including the specific areas accessed and changes made.	**GIG1**
GIS-8.2	**Firewall Security**	
GIS-8.2.1	All communications, including remote access, must pass through at least one approved application-level firewall. This includes connections to and from any non-system hosts used by the Gaming Enterprise.	**GIG1**
GIS-8.2.2	The firewall must be located at the boundary of any two dissimilar security domains.	**GIG1**
GIS-8.2.3	A device in the same broadcast domain as the system host must not have a facility that allows an alternate network path to be established that bypasses the firewall.	**GIG2**
GIS-8.2.4	Any alternate network path existing for redundancy purposes must also pass through at least one application-level firewall.	**GIG1**
GIS-8.2.5	Only firewall-related applications may reside on the firewall.	**GIG1**
GIS-8.2.6	The user accounts on the firewall must be limited (e.g., network or system administrators only).	**GIG1**
GIS-8.2.7	The firewall must reject all connections except those that have been specifically approved.	**GIG1**
GIS-8.2.8	The firewall must reject all connections from destinations which cannot reside on the network from which the message originated (e.g., RFC1918 addresses on the public side of an internet firewall).	**GIG1**
GIS-8.2.9	The firewall must only allow remote access using encryption.	**GIG1**
GIS-8.2.10	The firewall must be able to log the following information in an audit log in a manner which preserves and secures the information from loss or alteration: a. All changes to configuration of the firewall; b. All successful and unsuccessful connection attempts through the firewall; and c. The source and destination IP Addresses, Port Numbers, Protocols, and where possible, MAC Addresses.	**GIG1**
GIS-8.2.11	For unsuccessful connection attempts through the firewall, a configurable parameter may be utilized to deny further connection requests, and notify the system administrator, should the predefined threshold be exceeded.	**GIG1**
GIS-9	**Critical Asset and Change Management Review**	**GIG**
GIS-9.1	**Asset Management**	
GIS-9.1.1	All physical or logical assets housing, processing, or communicating sensitive data, including those comprising the GPE, must be accounted for.	**GIG1**
GIS-9.1.2	Procedures must exist for adding new assets and removing assets from service.	**GIG1**
GIS-9.1.3	A policy must be included on the acceptable use of assets associated with the GPE.	**GIG1**
GIS-9.1.4	The designated owner of each asset must: a. Ensure that information and assets are appropriately classified based on their confidentiality, integrity, accountability, and availability requirements; and b. Define access restrictions and classifications based on the established classification criteria and the principle of least privilege.	**GIG1**
GIS-9.1.5	A procedure must exist to ensure that recorded accountability for assets is compared with actual assets at least annually or at intervals required by the Regulatory Body and appropriate action is taken with respect to discrepancies.	**GIG1**
GIS-9.1.6	Copy protection to prevent unauthorized duplication or modification of licensed software may be implemented provided that: a. The method of copy protection is fully documented and 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.	**GIG1**

GIS-9.1.7	To ensure its continued availability integrity, and confidentiality of information, assets must be correctly maintained, inspected, and serviced at least annually or at regular intervals required by the Regulatory Body to ensure that it is free from defects or mechanisms that could interfere with its operation.	**GIG1**
GIS-9.1.8	Storage media must be managed through their lifecycle of acquisition, use, transportation, and disposal in accordance with the Gaming Enterprise's classification scheme and handling requirements.	**GIG1**
GIS-9.1.9	Assets must be disposed of securely and safely using documented procedures.	**GIG1**
GIS-9.1.10	Sensitive data stored in Critical System Components, devices or in any other storage media must be deleted when no longer required.	**GIG1**
GIS-9.1.11	Prior to disposal or re-use, assets containing storage media must be checked to ensure that any licensed software, as well as sensitive data has been removed or securely overwritten (i.e., not just deleted).	**GIG1**
GIS-9.2	**Critical Asset Register (CAR)**	
GIS-9.2.1	A CAR must be developed and maintained for any assets that affect the functionality of the GPE or has an influence on how sensitive data is stored/handled by the environment.	**GIG1**
GIS-9.2.2	The structure of the CAR must include hardware and software components and the inter-relationships and dependencies of the components.	**GIG1**
GIS-9.2.3	The following minimum items must be documented in the CAR for each asset: a. A unique ID that is assigned to each individual asset; b. The name/definition of each asset; c. A version number of the asset listed; d. Identifying asset characteristics (e.g., system component, database, virtual machine, hardware); e. The "owner" responsible for the asset; f. The geographical location of hardware assets; and g. Relevance codes on the asset's role in achieving or ensuring the classification criteria.	**GIG1**
GIS-9.2.4	The classification criteria is as follows: a. Confidentiality of sensitive data (e.g., identification and transaction information); b. Integrity of the system, specifically any asset that affects the functionality of the system and/or has an influence on how sensitive data is stored and/or handled; c. Availability of sensitive data; and d. Accountability of user activity, and how much influence the asset has on the user activity.	**GIG1**
GIS-9.2.5	Each of the classification criteria must be assigned a relevance code of: a. 1 - No Relevance: The asset can have no negative impact on the criteria; b. 2 - Some Relevance: The asset can have an impact on the criteria; or c. 3 - Substantial Relevance: The criteria are related to or dependent on the asset.	**GIG1**
GIS-9.3	**Change Management**	
GIS-9.3.1	A CMP must be implemented for handling updates to the GPE and its Critical System Components based on the propensity for frequent system upgrades and chosen risk tolerance. For a GPE that requires frequent updates, a risk-based CMP may be utilized to afford greater efficiency in deploying updates. Risk-based CMPs typically include a categorization of proposed changes based on regulatory impact and define associated certification procedures for each category.	**GIG1**
GIS-9.3.2	Program change procedures must be adequate to ensure that only authorized versions of programs and modifications are implemented in the GPE.	**GIG1**
GIS-9.3.3	An appropriate software version control mechanism must be in place for all software components, source code, and binary controls.	**GIG1**
GIS-9.3.4	A CML must be kept of all new installations and/or modifications to the system, including: a. The date of the installation or modification; b. Details of the reason or nature of the installation or change such as new software, server repair, significant configuration modifications; c. The component(s) to be changed including the unique identification number from the CAR, version information, and if the component being changed is hardware, the physical location of this component; d. The identity of the user(s) performing the installation or modification; and e. The identity of the user(s) responsible for authorizing the installation or modification.	**GIG1**

GIS-9.3.5	A strategy must be in place to cover the potential for an unsuccessful install or a field issue with one or more changes implemented: a. Where an outside party such as an App store is a stakeholder in the release process, this strategy must cover managing releases through the outside party. This strategy may consider the severity of the issue. b. Otherwise, this strategy must cover reverting back to the last implementation (rollback plan), including complete backups of previous versions of software and a test of the rollback plan prior to implementation to the GPE.	**GIG1**
GIS-9.3.6	A policy addressing emergency change procedures must be in place. Emergency changes must be approved, tested, documented, and monitored.	**GIG1**
GIS-9.3.7	Procedures must be in place for testing and migration of changes, including the identification of authorized personnel for signoff prior to release.	**GIG1**
GIS-9.3.8	There must be segregation of duties within the release process.	**GIG1**
GIS-9.3.9	Technical and user documentation must be maintained, such as manuals and user guides, describing the systems in use and the operation, including hardware.	
GIS-9.3.10	Procedures must be in place to ensure that technical and user documentation is updated as a result of a change.	**GIG1**
GIS-9.4	**System Development Lifecycle**	
GIS-9.4.1	The acquisition and development of new software must follow defined processes established by the Gaming Enterprise and/or Regulatory Body.	**GIG1**
GIS-9.4.2	The GPE must be logically and physically separated from the development and testing environments such that no direct connection may exist between the GPE and any other environment.	**GIG1**
GIS-9.4.3	The delegation of responsibilities must be established where applicable.	**GIG1**
GIS-9.4.4	The Gaming Enterprise must establish and document a method for developing software securely, which includes following industry standards and best practices for coding.	**GIG1**
GIS-9.4.5	GIS considerations must be integrated throughout the software development lifecycle, from initial requirements gathering to deployment and maintenance.	**GIG1**
GIS-9.4.6	The documented test methodology must include provisions to a. Verify that test software is not deployed to the GPE; b. Appropriately select, protect, and manage test data; and c. Prevent the use of actual sensitive data or other raw production data in testing.	**GIG1**
GIS-9.4.9	All documentation relating to software and application development must be available and retained for the duration of its lifecycle.	**GIG1**
GIS-9.5	**Patch Management**	
GIS-9.5.1	The Gaming Enterprise must have patch management policies approved by the Regulatory Body, whether developed and supported by the Gaming Enterprise.	**GIG1**
GIS-9.5.2	The Gaming Enterprise must monitor and apply patches to all Critical System Components involved in the collection, processing, storage, and transmission of sensitive data.	**GIG1**
GIS-9.5.3	Whenever possible, all patches must be tested on a development and testing environment configured identically to the target GPE.	**GIG1**
GIS-9.5.4	Under circumstances where patch testing cannot be thoroughly conducted in time to meet the timelines for the severity level of the alert, then patch testing must be risk managed, either by isolating or removing the untested component from the network or applying the patch and testing after the fact.	**GIG1**

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

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.
Address Resolution Protocol (ARP)	The protocol used to translate IP addresses into MAC addresses to support communication on a wireless or wired local area network.
Administrative Controls	Policies, procedures, and guidelines implemented by a Gaming Enterprise to manage its GISMS.
Advanced Encryption Standards (AES)	A symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.
Algorithm	A finite set of unambiguous instructions performed in a prescribed sequence to achieve a goal, especially a mathematical rule or procedure used to compute a desired result. Algorithms are the basis for most computer programming.
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.
Backup	A copy of files and programs made to facilitate recovery if necessary.
Biometrics	A biological identification input, such as fingerprints, retina patterns, facial recognition data, or voiceprints
Bridge	Divides networks to reduce overall network traffic. A bridge allows or prevents data from passing through it by reading the MAC address.
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 security incident response purposes
Business Continuity and Disaster Recovery Plan	A plan for processing critical applications and preventing loss of data in the event of a major hardware or software failure or destruction of facilities.
Cache Poisoning	An attack where the attacker inserts corrupt data into the cache database of the Domain Name Service (DNS).
Communications Technology	Any method used, and the components employed, to facilitate the transmission and receipt of information, including transmission and reception by systems using wire, wireless, cable, radio, microwave, light, fiber optics, satellite, or computer data networks, including the Internet and intranets.
Compliant	The policy and evidence viewed was considered to be fully compliant with the GLI-GSF.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Contingency Plan	Management policy and procedures designed to maintain or restore gaming operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
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.

Term	Descriptions
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. • 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 System (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
Cryptographic Module	Hardware, software, firmware, or combination thereof that implement cryptographic functions such as encryption, decryption, signatures, hashing, and key management. The primary purpose of a cryptographic module is to provide secure processing and storage of keys and operations.
Data Integrity	The property that data is both accurate and consistent and has not been altered in an unauthorized manner in storage, during processing, and while in transit.

Term	Descriptions
Distributed Denial-of-Service (DDoS)	A type of attack where multiple compromised systems, usually infected with a destructive software program, are used to target a single system. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.
Domain	A group of computers and devices on a network that are administered as a unit with common rules and procedures.
Domain Name Service (DNS)	The globally distributed internet database which (amongst other things) maps machine names to IP numbers and vice-versa.
Dynamic Host Configuration Protocol (DHCP)	A network service that allows devices to request a configuration from a central point. First a request is broadcasted over the network segment, then any servers respond to that specific machine with an address, how long that address is good for, and other pertinent details.
Effective Bandwidth	The amount of data that actually can be transferred across a network per unit of time. The effective bandwidth through the Internet is usually considerably lower than the bandwidth of any of the constituent links.
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.
Encryption Key	A key that has been encrypted in order to disguise the value of the underlying plaintext.
Externally-Exposed Applications	Applications that are public facing and discoverable through reconnaissance and network scanning from the public internet outside of the enterprise's network. This does not apply to applications intended for patron use.
Externally-Exposed Enterprise Assets	Assets that are public facing and discoverable through Domain Name System reconnaissance and network scanning from the public internet outside of the enterprise's network. This does not apply to assets intended for patron use.
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 integrity, confidentiality, and availability.
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, 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.
Gateway	Any device, system, or software application that can perform the function of translating data from one format to another. The key feature of a gateway is that it converts the format of the data, not the data itself.
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.
GIS Incident	An occurrence that actually or potentially jeopardizes the integrity, confidentiality, or availability of a GPE or the sensitive data the GPE processes, stores, or transmits or that constitutes a violation or imminent threat of violation of GIS policies or procedures, or acceptable use policies.

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

Term	Descriptions
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
Group Membership	A method of organizing user accounts into a single unit (by job position) whereby access to system functions may be modified at the unit level and the changes take effect for all user accounts assigned to the unit.
Hash Algorithm	A function that converts a data string into an alpha-numeric string output of fixed length.
Hypertext Transport Protocol (HTTP)	The underlying protocol used to define how messages are formatted and transmitted, and what actions servers and browsers must take in response to various commands.
Hub	Connects devices on a twisted-pair network. A hub does not perform any tasks besides signal regeneration.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Internet	An interconnected system of networks that connects computers around the world via TCP/IP.
Internet Protocol Address (IP Address)	A unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.
Intrusion Detection System/Intrusion Prevention System (IDS/IPS)	A system that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Used in computer security, intrusion detection refers to the process of monitoring computer and network activities and analyzing those events to look for signs of intrusion in the GPE.
IP Security (IPSec)	A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of encryption keys to be used during the session.
Kerberos	A network authentication protocol designed to provide strong authentication for client/server applications by using secret-key encryption.
Key	A value used to control cryptographic functions, such as decryption, encryption, decryption, signatures, hashing etc.
Key Management	Activities involving the handling of encryption keys and other related security parameters (e.g., passwords) during the entire lifecycle of the keys, including their generation, storage, establishment, entry, and output, and zeroization.
Link Utilization	The percentage time that a communications link is engaged in transmitting data.
Major Non-Conformity	A fundamental failing (systematic) has been identified that affects several GIS Controls and means that the overall GIS policies cannot be adhered to. It may be either: • A number of minor non-conformities against one control can represent a total failure of the system and thus be considered a major non-conformity; • Any non-conformity that would result in the probable shipment of a non-conforming product. A condition that may result in the failure or materially reduce the usability of the products or services for their intended purpose; or • A non-conformity that judgment and experience indicate is likely either to result in the failure of the system or to materially reduce its ability to assure controlled processes and products.
Malfunction	When a Critical System Component does not operate as intended.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the integrity, confidentiality, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Term	Descriptions
"Man-In-The-Middle" Attack	An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
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.
Minor Non-Conformity	A GIS Control has not been addressed or is not compliant with the GLI-GSF (non-systematic) and that judgment and experience indicate is not likely to result in the failure of the system or reduce its ability to assure controlled processes or products. It may be either: • A failure in some part of the system relative to a control; or • A single observed lapse in following one item of the system.
Mobile Code	Executable code that moves from computer to computer, including both legitimate code and malicious code such as computer viruses.
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).
Network Communication Equipment (NCE)	Communications technology that controls data communication in a system including, but not limited to, NICs, cables, switches, bridges, hubs, routers, wireless access points, and telephones, VoIP network devices, wireless access points, network appliances, and other security appliances.
Network Interface Card (NIC)	The mechanism by which terminals and systems connect to the network. NICs can be add-in expansion cards, PCMCIA cards, or built-in interfaces.
Observation	A finding worth noting for possible improvement to meet industry best practices.
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.
Personal Identification Number (PIN)	A numerical code associated with an individual and which allows secure access to a domain, account, network, system, etc.
Physical and Environmental Controls	The measures implemented to protect physical assets, facilities, and environmental conditions that house the Gaming Production Environment's systems and infrastructure.
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).
Proxy	An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks.
Protocol	A set of rules and conventions that specifies 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.

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

Term	Descriptions
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.
Router	Connects networks together. A router uses the software-configured network address to make forwarding decisions.
Secure Communication Protocol	A communication protocol that provides the appropriate confidentiality, authentication, and content integrity protection.
Secure Shell (SSH)	Allows tunneling any other protocol in a secure manner.
Security Certificate	Information, often stored as a text file that is used by the Transport Socket Layer (TSL) Protocol to establish a secure connection. In order for a TSL connection to be created, both sides must have a valid Security Certificate.

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.
Service Set Identifier (SSID)	A name that identifies a particular 802.11 wireless LAN.
Shellcode	A small piece of code used as a payload in the exploitation of security. Shellcode exploits vulnerability and allows an attacker the ability to reduce a system’s information assurance.
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).

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.

Term	Descriptions
Social Engineering	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. Social engineering attacks include non-technical intrusions into a GPE using information acquired through human interaction and rely on tricks that prey on an individual being unfamiliar with emerging technology and protocols.
Source Code	A text listing of commands to be compiled or assembled into an executable computer program.
Stateless Protocol	A communications scheme that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses.
Switch	Connects devices on an 802.3 network. A switch forwards data to its destination by using the MAC address embedded in each packet.
System Administrator	The individual(s) responsible for maintaining the stable operation of the GPE (including software and hardware infrastructure and application software).
Technical Controls	The security mechanisms implemented within Gaming Production Environment's systems and infrastructure to protect against unauthorized access, data breaches, and other security threats.
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 DoS; 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.
Time Stamp	A record of the current value of the date and time which is added to a message at the time the message is created.
Transmission Control Protocol/Internet Protocol (TCP/IP)	The suite of communications protocols used to connect hosts on the Internet.
Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
User Datagram Protocol (UDP)	A transport protocol that does not guarantee delivery. Thus, it is faster, but less reliable.
Version Control	The method by which evolving approved Critical System Components are verified to be operating in an approved state.
Virtual Private Network (VPN)	A logical network that is established over an existing physical network and which typically does not include every node present on the physical network.
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.
Wired Equivalent Protocol (WEP)	An easily broken and therefore deprecated algorithm to secure IEEE 802.11 wireless networks. It was originally intended to allow the same level of protection as a wired connection, but flaws were soon discovered after its adoption that made it barely better than no protection at all.
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.
Wi-Fi	The standard wireless local area network (WLAN) technology for connecting computers and electronic devices to each other and/or to the internet.
Wi-Fi Protected Access (WPA)	The successor to WEP. Its authentication can be broken under certain circumstances, but sufficiently complex passphrases are secure enough for most uses.
Workstation	An interface for authorized personnel to access the regulated functions of the GPE.

Copyright © 2025 Gaming Laboratories International, LLC

All Rights Reserved.