GLI®

Gaming Security Framework

GLI-GSF-1

Gaming Information Security (GIS) Common Controls Audit

Version 1.0 DRAFT – Published July 30, 2024

Gaming Laboratories International®

Contents

1. INTRODUCTION

1.1. General Statement

The integrity and accuracy of the operation of a Gaming Production Environment (GPE) is highly dependent upon operational procedures, configurations, and the network infrastructure. With ever emerging threats to gaming operations, regulatory bodies rely heavily on the expertise of a qualified Independent Security Firm (ISF) to perform gaming security assessments as an essential addition to the testing and certification of the Critical System Components of a GPE by an Independent Test Laboratory (ITL). This module of the GLI Gaming Security Framework, GLI-GSF-1, sets forth the gaming information security (GIS) common controls necessary for auditing a Gaming Enterprise's Gaming Information Security Management System (GISMS) to ensure effective management of security in a Gaming Enterprise's GPE. These GIS common controls apply to GPEs used for all forms of gaming, such as casino gaming, lottery, event wagering, and interactive gaming. 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 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:

a. Critical System Components: This includes the 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.

1.3. 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.

1.4. 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 shall 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.

2. GIS AUDITS

2.1. Audit Overview

The GIS 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 approach relies heavily on layered security to reduce the risk to computer and network systems. The layered approach provides redundancy and reinforces the overall security model, as several layers of security shall be breached before a critical 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 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, suggested audit activities. The Appendix details the minimum GIS common control requirements 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

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 information and other critical assets. The following key personnel responsible for establishing the GIS policy and applying shall be interviewed at a minimum.

a. Person with overall responsibility for the gaming operation
b. Compliance officer
c. Information security officer
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 / Penetration Testing
c. Network and Communications Security
d. Logical Access Controls
e. Operating Systems (OS) Security
f. Malicious Software Controls

g. Database Design and Configuration
h. Cryptographic Controls
i. System Monitoring
j. Reporting and Logging
k. 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 issues of non-conformance to any applicable 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.

2.4. Audit Frequency

2.4.1. Initial Audit

The Gaming Enterprise shall have a GIS 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 this audit as requested by the Gaming Enterprise, along with an updated audit schedule, shall be authorized by the regulatory body.

NOTE: It is recommended for regulatory bodies to allow flexibility for 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 shall, as a rule, have another GIS audit performed by an ISF within twelve months of the previous GIS audit unless the regulatory body has advised otherwise. Any postponement of this audit as requested by the Gaming Enterprise, along with an updated audit schedule, shall be authorized by the regulatory body.

NOTE: It is recommended for regulatory bodies to allow flexibility for audit schedules for multi-jurisdictional Gaming Enterprises to allow consolidation of audits for multiple jurisdictions to a common schedule.

2.4.3. Additional Audits

Additional GIS audits may be needed more frequently based on the critically of changes within the GPE, such as additions and/or changes which may affect or provide access to sensitive data and/or Critical System

Components. Such GIS audits, as required by the regulatory body and/or the Gaming Enterprise, may be focused on specific functions of, additions to, and/or changes to the GPE.

2.5. GIS Audit Reports

The results of a GIS audit will identify for management those areas in the operations where improvement should be considered and recommend strategies for improving those areas. The GIS audit report shall be submitted to the regulatory body no later than sixty days after the GIS audit has been completed. The GIS audit report shall include all the following:

a. The name and a brief background of the Gaming Enterprise, mentioning its business model and gaming activities offered or Service Providers used, as well as the location, number of employees, website, actual certifications, high level description of the infrastructure including data center, etc.
b. The ISF's name, company affiliation, contact information, and qualifications and experience of the individuals who conducted the audit;
c. The date(s) of the audit, including the request date, the start date, the completion date, the report date, and the expiration date;
d. The scope of the audit, including:
    i. A high level overview of the work undertaken and the control environment operating;
    ii. The controls against which the audit was conducted;
    iii. The Critical System Components that were reviewed
    iv. How the Critical System Components were identified and if the audit included applications, networks, databases, and/or operating systems;
    v. An indication of any conditions of the audit, including the controls excluded from audit and the reasons for their exclusion;
e. The audit approach, including enquiry-based questions, observation, evidence, key persons interviewed;
f. Evidence obtained during the audit to substantiate audit results, including:
    i. The documents that were reviewed, including version and dates, staff interviewed;
    ii. The names, dates, and versions of documentation reviewed;
    iii. The names, roles, and locations of personnel interviewed;
    iv. The locations visited;
    v. The details of the walkthroughs performed;
    vi. The samples reviewed to verify compliance;
g. The results of the audit, indicating for each control its status as compliant, observation, minor non-conformity, or major non-conformity;
h. Findings, including:
    i. An explanation of the non-conformities identified;
    ii. Evidence that supports and describes the non-conformities;
    iii. Impact or potential impact of the non-conformities;
    iv. Recommended corrective actions to be taken to address existing non-conformities and make improvements;
i. The Gaming Enterprise's response to the findings and recommended corrective action, including resolution dates and responsible persons; and
j. Other relevant factors, such as whether the GISMS are compliant or have been audited against other requirements (e.g. ISO/IEC 27001, WLA-SCS, NIST-CSF, etc.)

2.6. Corrective Actions

If the ISF's GIS audit report recommends corrective action, the Gaming Enterprise shall provide the ISF and the regulatory body with a remediation plan and any risk mitigation plans which detail the Gaming Enterprise's actions and schedule to implement the corrective action.

a. Non-conformities shall be addressed through the Gaming Enterprise's corrective action process, including:
    i. Actions taken to determine the extent of and contain the specific non-conformance.
    ii. Root cause investigation to determine the most basic causes of the non-conformance.
    iii. Actions taken to correct the non-conformance and, in response to the root cause, to eliminate

recurrence of the non-conformance.

b. Corrective actions to address the identified major non-conformities shall be carried out immediately and the ISF and the regulatory body shall be notified of the actions taken within thirty days, unless otherwise specified by the regulatory body. The ISF shall perform a follow up audit within ninety days to confirm the actions taken, evaluate their effectiveness, and determine whether the non-conformities have been resolved.

c. Corrective actions to address identified minor non-conformities shall be documented and sent by the Gaming Enterprise to the ISF and the regulatory body for review within thirty days, unless otherwise specified by the regulatory body. If the actions are deemed satisfactory, they will be followed up at the next scheduled audit.

d. Once corrective actions have been taken, the Gaming Enterprise will provide the ISF and the regulatory body with documentation evidencing completion.

e. The Gaming Enterprise shall maintain corrective action records, including objective evidence, for at least five years, unless otherwise specified by the regulatory body.

2.7. Independent Security Firm (ISF)

The GIS audit shall be carried out by individuals with sufficient qualifications, which means that the ISF shall hire sufficiently qualified, competent, and experienced individuals. These individuals shall:

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 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 GIS audits within the gaming industry; and

d. Meet any other qualifications as prescribed by the regulatory body.

NOTE: Nothing herein is intended to prohibit the regulatory body staff from acting as an ISF, provided they meet the requirements of this section, and they are independent from the Gaming Enterprise being audited.

APPENDIX: GAMING INFORMATION SECURITY (GIS) CONTROLS

The Gaming Information Security (GIS) Controls, as specified in this Appendix, will indicate which Gaming Implementation Group (GIG) the 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 shall address availability of services and the integrity and confidentiality of sensitive data. Successful attacks can cause significant harm to public welfare. GIS Controls selected for GIG3 shall 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.

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 shall 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-8.10	Retain 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

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

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

B. Additional GIS Common 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 System Component Functions	GIG
GIS-1.1	**GPE Internal Clock**	
GIS-1.1.1	The GPE shall maintain an internal clock that reflects the current date and time which shall be used to provide for the time stamping of all transactions, configuration changes, and significant events, and as a reference clock for reporting.	**GIG1**
GIS-1.1.2	Changes to the internal clock's date and time, or the approved time sources, shall be recorded in a 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 System Component Verification**	
GIS-1.2.1	The Critical System Components of the GPE shall be verified as identical to those approved by the regulatory body via a signature verification procedure, which shall 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-1.2.2	The signature verification procedure shall: 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 shall be reviewed on a case-by-case basis. c. Include one or more analytical steps to compare the current signatures of the Critical System Components in the GPE with the signatures of the current approved versions of the Critical System Components.	**GIG1**
GIS-1.2.3	The output of the signature verification procedure shall be recorded in a system log, which shall a. Detail the following for each verification: i. The date and time of the verification; ii. Identification of each verified Critical System Component; iii. The expected and generated signature results, including indication of any program error or signature mismatch; iv. When performed on demand, user account ID who initiated the verification procedure; b. Be accessible by the regulatory body in a format which will permit analysis of each verification by the regulatory body; and c. Comprise part of the sensitive data which shall be recovered in the event of a disaster or equipment or software failure.	**GIG1**
GIS-1.2.4	Any failure of signature verification of any Critical System Component shall require a notification of the verification failure being communicated to the Gaming Enterprise and regulatory body as required.	**GIG1**
GIS-1.2.5	There shall 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 System Component 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 shall 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 shall have a provision requiring review at planned intervals 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 shall be approved by management and communicated to and acknowledged by relevant Gaming Enterprise personnel and relevant Service Provider personnel.	**GIG1**
GIS-2.1.4	The GIS policy shall delineate the security roles and responsibilities of Gaming Enterprise personnel and relevant Service Provider personnel for the operation, service, and maintenance of the GPE.	**GIG1**
GIS-2.2	**Access Control Policy**	
GIS-2.2.1	An access control policy shall be established and documented which shall be periodically reviewed based on business and security requirements for physical and logical access to the GPE, including remote access as allowed by the regulatory body.	**GIG1**
GIS-2.2.2	A formal user registration and de-registration procedure shall be in place for granting and revoking access to the GPE.	**GIG1**
GIS-2.2.3	The allocation and use of user access rights and privileges shall be restricted and controlled based on business requirements and the principle of least privilege.	**GIG2**
GIS-2.2.4	Personnel shall only be provided with access to the services or facilities that they have been specifically authorized to use.	**GIG1**
GIS-2.2.5	Management shall review and confirm user access rights and privileges at regular intervals using a formal process.	**GIG2**
GIS-2.3	**Allocation of Security Responsibilities**	
GIS-2.3.1	Security responsibilities shall be effectively documented and implemented.	**GIG2**
GIS-2.3.2	A security forum comprised of management shall 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 periodically as required by the regulatory body.	**GIG2**
GIS-2.3.3	A security function shall exist that will be responsible for developing and implementing security strategies and action plans.	**GIG2**
GIS-2.3.4	The security function shall be involved in and review all processes regarding security aspects of the Gaming Enterprise, including, but not be limited to, the protection of information, communications, physical infrastructure, and gaming processes.	**GIG2**
GIS-2.3.5	The security function shall report to no lower than senior management and not reside within or report to the IT function.	**GIG2**
GIS-2.3.6	The security function shall have the competences and be sufficiently empowered and have access to all necessary resources to enable adequate assessment, management, and reduction of risk.	**GIG2**
GIS-2.3.7	The head of the security function shall be a member of the security forum and be responsible for recommending security policies and changes.	**GIG2**
GIS-2.4	**Personally Identifiable Information (PII) Privacy**	
GIS-2.4.1	Any PII obtained in respect to the patron shall be protected in compliance with the privacy policy and local privacy regulations and standards observed by the regulatory body, as well as contractual requirements.	**GIG1**
GIS-2.4.2	Any PII which is not subject to disclosure pursuant to the privacy policy shall be kept confidential, except where the release of that information is required by law.	**GIG1**
GIS-2.4.3	There shall be procedures in place for the security, sharing, and controlled usage of PII as required by the regulatory body.	**GIG1**
GIS-2.4.4	The Gaming Enterprise shall designate one or more individuals with primary responsibility for the design, implementation, and ongoing evaluation of procedures and practices related to the security and sharing of PII.	**GIG1**
GIS-2.4.5	Procedures shall be established to determine the nature and scope of all PII collected by the Gaming Enterprise, including the types of information collected, sources of collection, and purposes of use.	**GIG1**
GIS-2.4.6	Where required by the regulatory body, patrons shall be provided with a method to request confirmation of PII processing, access to a copy of their PII and related processing information, updates to their PII, and erasure or processing restrictions of their PII. a. Procedures shall be in place to record and process these requests, maintain records of them, and provide reasons for any denial or rejection. b. Patrons shall be informed when the Gaming Enterprise does not intend to comply with their request and given information on filing a complaint with the regulatory body.	**GIG1**

GIS-2.4.7	Where required by the regulatory body and upon patron's request, the Gaming Enterprise shall forward to the patrons the PII which they have received from the same patron, in a structured, commonly used, and machine-readable format and transmit the PII to another Gaming Enterprise, where it is technically feasible to do so. This only applies to: a. PII which the patron has provided to the Gaming Enterprise or PII which is processed by automated means (i.e., this would exclude any paper records); and b. Cases where the basis for processing is PII consent, or that the data is being processed to fulfil a contract or steps preparatory to a contract.	**GIG1**
GIS-2.4.8	Where required by the regulatory body, the patron has the right to object to PII processing: a. Based on legitimate interests or the performance of a task in the public interest or in the exercise of official authority; b. Used in direct marketing, including profiling to the extent that it is related to such marketing activities; and c. For scientific or historical research purposes or for the purpose of statistics.	**GIG1**
GIS-2.4.9	There shall be procedures in place for the Gaming Enterprise to comply with requests from patrons to have PII erased and/or to prevent or restrict processing of PII, including, in the following circumstances: a. Where the PII is no longer necessary in relation to the purpose for which it was originally collected/processed; b. When the patron withdraws consent; c. When the patron objects to the PII processing and there is no overriding legitimate interest for continuing the processing; d. The PII was unlawfully processed; or e. The PII shall be erased in order to comply with a legal obligation.	**GIG1**
GIS-2.4.10	Where prohibited by the regulatory body, the Gaming Enterprise may not utilize solely automated decision-making which: a. Produces legal effects the patron such as those which result in the patron being subjected to surveillance by a competent authority; or b. Significantly affects the patron in a similar manner (e.g., it has the potential to influence the circumstances, behavior, or choices of the patron).	**GIG1**
GIS-2.5	**Securing Financial Transactions within the GPE**	
GIS-2.5.1	Payment methods used for financial transactions in the GPE shall be protected from fraudulent use.	**GIG1**
GIS-2.5.2	The collection of sensitive data directly related to each financial transaction within the GPE shall be limited to only the sensitive data strictly needed for the transaction.	**GIG1**
GIS-2.5.3	There shall 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 shall 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 shall 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 shall monitor and adjust resource capacity and consumption to ensure availability is maintained.	**GIG1**
GIS-3.1.3	The Gaming Enterprise shall maintain a log of the system performance, including a function to compile performance reports.	**GIG2**
GIS-3.1.4	The Gaming Enterprise shall 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 shall establish procedures to gather and analyze threat intelligence, and to act on it appropriately.	**GIG2**

GIS-3.2	**GPE Malfunctions**	
GIS-3.2.1	Upon detection of a malfunction, the Gaming Enterprise shall initiate an investigation to determine the root cause of the malfunction.	**GIG1**
GIS-3.2.2	The investigation shall involve a thorough review of relevant records, reports, 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 shall 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 shall be conducted to ensure its integrity and functionality.	**GIG1**
GIS-3.2.5	The Gaming Enterprise shall 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 shall 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 shall 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, the regulatory body, affected users, and other relevant authorities shall be notified. The notification shall include 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 shall include documented procedures to handle various types of GIS incidents.	**GIG1**
GIS-3.3.5	Procedures shall be established for the controlled recovery from GIS incidents, including restoring affected systems and sensitive data to a known good state.	**GIG1**
GIS-3.4	**Physical Location of Servers**	
GIS-3.4.1	The GPE servers, sensitive data, information, and other associated assets shall 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 shall have sufficient protection against alteration, tampering or unauthorized access.	**GIG1**
GIS-3.4.3	Each secure location shall be equipped with a surveillance system that shall meet the procedures put in place by the regulatory body.	**GIG1**
GIS-3.4.4	Security measures for working in secure locations shall be designed and implemented.	**GIG1**
GIS-3.4.5	Security perimeters shall be defined and used to protect each secure location.	**GIG1**
GIS-3.4.6	Each secure location shall be protected by appropriate entry controls to ensure that access is restricted to only authorized personnel. MFA shall be used for physical access unless the secure location is staffed at all times.	**GIG1**
GIS-3.4.7	Access devices to the secure location, such as magnetic swipe, proximity cards, embedded chip cards, fobs, keys, shall be controlled by authorized personnel.	**GIG1**
GIS-3.4.8	All attempts at physical access to each secure location shall be recorded in a 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-3.4.9	Each secure location shall 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-3.4.10	The GPE shall be protected from power failures and other disruptions caused by failures in supporting utilities.	**GIG1**
GIS-3.4.11	Cables carrying power, data or supporting Critical System Components shall be protected from interception, interference, or damage.	**GIG1**
GIS-3.4.12	All Critical System Components shall be provided with adequate primary power.	**GIG1**

GIS-3.4.13	Where the server is a stand-alone application, it shall have an Uninterruptible Power Supply (UPS) connected and shall 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 shall be in use if not incorporated into the UPS itself.	**GIG1**
GIS-3.5	**Logical Access Control**	
GIS-3.5.1	The GPE shall 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 shall have their own individual authentication credential whose provision shall be controlled through a formal process.	**GIG1**
GIS-3.5.3	Users shall only have access to the functionality and features appropriate for their role and responsibilities within the system.	**GIG1**
GIS-3.5.4	It shall 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 shall be recorded in a 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 shall be limited, and where used the reasons for their use shall be formally documented.	**GIG1**
GIS-3.5.6	Authentication credential records for secret information shall 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 shall 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) shall be at least as strong as the primary method. An MFA process shall be employed for these purposes.	**GIG2**
GIS-3.5.9	Lost or compromised authentication credentials and authentication credentials of terminated users shall be deactivated, secured, or destroyed as soon as reasonably possible.	**GIG1**
GIS-3.5.10	The system shall 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 shall 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 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 shall be: a. Restricted through logical security 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 shall 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 shall be recorded in a 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 shall 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 shall be recorded in a 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 shall 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**
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 shall 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 shall 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 shall be documented and shall 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 shall 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 shall always be created randomly, in memory, and shall 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 shall be used to provide additional security for high-risk applications, such as remote access.	**GIG1**
GIS-3.6.7	If the system does not receive input from the individual within five minutes, or a period specified by the regulatory body, the user session shall time out or lock up, requiring the personnel to re-establish their authorization to continue.	**GIG1**
GIS-3.7	**Server Programming**	
GIS-3.7.1	The GPE shall be sufficiently secure to prevent any 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 shall 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	Redundant server instances shall not run under the same hypervisor.	**GIG2**

GIS-3.8.2	Each server instance may perform only one function.	**GIG2**
GIS-3.9	**Electronic Document Retention System (ERDS)**	
GIS-3.9.1	The ERDS shall be properly configured to maintain the original version along with all subsequent versions reflecting all changes to reports or logs that are stored in an alterable format.	**GIG1**
GIS-3.9.2	The ERDS shall maintain a unique signature for each version of the log, including the original.	**GIG1**
GIS-3.9.3	The ERDS shall retain a 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 shall provide a method of complete indexing for easily locating and identifying the log including at least the following (which may be input by the user): a. Date and time the log was generated; b. Critical system component generating the log; c. Title and description of the log; d. User account ID of who is generating the log; and e. Any other information that may be useful in identifying the log and its purpose.	**GIG1**
GIS-3.9.5	The ERDS shall be configured to a. Limit access to modify or add reports or logs to the system through logical security of specific user accounts; and b. Provide a log of all administrative user account activity.	**GIG1**
GIS-3.9.6	The ERDS shall 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 shall 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 shall 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	Appropriate data handling methods shall be implemented, including validation of input and rejection of corrupt sensitive data.	**GIG2**
GIS-4.1.3	The number of workstations where critical applications or associated databases may be accessed shall be limited.	**GIG1**
GIS-4.1.4	Encryption or equivalent security shall be used for files and directories containing sensitive data. If encryption is not used, the Gaming Enterprise shall restrict users from viewing the contents of such files and directories, which at a minimum shall 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	Alterations to the GPE's live data files and database tables occurring outside of normal program and operating system execution shall be recorded in a 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 shall 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 shall 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 shall 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 shall protect the confidentiality, integrity, accountability, and availability of sensitive data, when held at-rest on servers, critical applications, and associated databases containing sensitive data.	**GIG2**

GIS-4.1.11	Encryption shall 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 shall be authenticated shall use some form of message authentication technique.	**GIG2**
GIS-4.1.13	Authentication shall 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 shall reside on networks separated from the servers hosting any patron interfaces.	**GIG1**
GIS-4.1.15	Sensitive data shall 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 shall be applied to systems, networks and any other devices that process, store, or transmit sensitive data.	**GIG2**
GIS-4.1.17	Sensitive data shall 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 shall not be permitted without supervised access controls. In the event any sensitive data is changed, the following information shall 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**
GIS-4.1.19	Any irrecoverable loss of sensitive data shall be recorded in a 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-4.2	**Backup Process Implementation**	
GIS-4.2.1	Backup process implementation shall occur at least daily or as otherwise specified by the regulatory body, although all methods will be reviewed on a case-by-case basis.	**GIG1**
GIS-4.2.2	Sensitive data, critical applications, and associated databases shall 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 shall be kept on the GPE with open support for backups and restoration.	**GIG1**
GIS-4.2.4	The backup shall 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 shall 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 shall 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 shall be managed with at least the same level of security and access controls as the GPE.	**GIG1**
GIS-4.2.10	Backup data files and data recovery components shall be maintained, protected, and regularly tested in accordance with the agreed backup process.	**GIG2**
GIS-4.3	**System Failure and Recovery**	
GIS-4.3.1	Failure or significant periods of unavailability of a Critical System Component (any length of time operations is halted for all users, and/or transactions cannot be successfully completed for any user) shall be recorded in a 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-4.3.2	The GPE shall 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-4.3.3	When two or more Critical System Components are linked a procedure shall 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 shall 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 shall immediately synchronize the status of all transactions, sensitive data, and configurations with one another.	**GIG1**
GIS-4.3.6	The Gaming Enterprise shall 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 shall 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**
GIS-4.4.2	The business continuity and disaster recovery plan shall 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 shall address the method of storing sensitive data to minimize loss. If asynchronous replication is used, the method for recovering information shall be described or the potential loss of information shall be documented.	**GIG2**
GIS-4.4.4	The business continuity and disaster recovery plan shall delineate the circumstances under which it will be invoked.	**GIG1**
GIS-4.4.5	The business continuity and disaster recovery plan shall 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). Utilization of cloud platforms for this purpose will be evaluated on a case-by-case basis.	**GIG2**
GIS-4.4.6	The business continuity and disaster recovery plan shall 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 shall 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 shall be tested at least annually or as otherwise specified by the regulatory body. The results of the testing shall be documented.	**GIG1**
GIS-5	**Communications**	**GIG**
GIS-5.1	**Connectivity**	
GIS-5.1.1	Only authorized devices shall be permitted to establish communications between any Critical System Components.	**GIG1**
GIS-5.1.2	The GPE shall 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 shall be un-enrolled and disabled.	**GIG1**
GIS-5.1.5	The GPE shall log the establishment, loss, and reestablishment of communications between Critical System Components.	**GIG1**

GIS-5.2	**Communication Protocol**	
GIS-5.2.1	Each Critical System Component of the GPE shall function as indicated by a documented secure communication protocol.	**GIG1**
GIS-5.2.2	All protocols shall 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 will 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 shall employ encryption and authentication for integrity.	**GIG1**
GIS-5.2.4	Communications on the secure network shall 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 shall be allowed.	**GIG1**
GIS-5.2.5	Communications shall be hardened to be immune to all possible malformed message attacks.	**GIG1**
GIS-5.2.6	Failure of communications shall 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 shall not be established and authenticated until the program resumption routine, including any self-tests, is completed successfully.	**GIG1**
GIS-5.3	**Encrypted Tunneling Protocols**	

GIS-5.3.1	One of the following encrypted tunneling protocols or equivalent shall 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-5.3.2	The encrypted tunneling protocols shall 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-5.4	**Communications Over Internet/Public Networks**	
GIS-5.4.1	Communications between any Critical System Components which takes place over internet/public networks, shall 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-5.4.2	Sensitive data shall always be encrypted over the internet/public network and safeguarded from incomplete transmissions, misrouting, unauthorized message modification, disclosure, duplication, or replay.	**GIG1**
GIS-5.5	**Wireless Local Area Network (WLAN) Communications**	
GIS-5.5.1	Use of WLAN communications shall be secured and only used where appropriate and not in areas where it could be potentially harmful.	**GIG1**
GIS-5.5.2	Communications between wireless devices on the WLAN shall use protocols designed for securing, authenticating, and encrypting wireless networks.	**GIG1**
GIS-5.5.3	Multi-Factor Authentication (MFA) shall be required at the wireless network and device level.	**GIG1**
GIS-5.5.4	Authentication schemes using Public Key Infrastructure (PKI) shall require certificate validation, ideally in both directions (e.g. client certificates).	**GIG1**
GIS-5.5.5	Advance Encryption Standards (AES) or equivalent with a minimum of 256-bit encryption shall be used to support integrity and confidentiality services.	**GIG1**
GIS-5.5.6	The Pairwise Master Key (PMK) utilized shall 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 controls adopted by the Gaming Enterprise.	**GIG1**
GIS-5.5.7	The Group Master Key (GMK) utilized shall have a lifetime of eight hours or less.	**GIG1**

GIS-5.5.8	Wired Equivalent Privacy (WEP) shall 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 will be considered on a case-by-case basis.	**GIG1**
GIS-5.6	**Wireless Access Points (WAP)**	
GIS-5.6.1	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-5.6.2	The default administration login and password shall be changed from the factory default to a secure value controlled according to the Gaming Enterprise.	**GIG1**
GIS-5.6.3	The default network password shall be changed from the factory default to a secure value controlled according to the Gaming Enterprise.	**GIG1**
GIS-5.6.4	The SSID shall 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-5.6.5	Access to the administrative functions of the WAP shall 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-5.6.6	If the router supports WPA2 authentication, all WAPs shall be IEEE 802.11 compliant and configured with Enterprise Mode enabled or with a strong pre-shared key.	**GIG1**
GIS-5.7	**Network Communication Equipment (NCE)**	
GIS-5.7.1	The Gaming Enterprise shall provide a secure location for the placement, operation, and usage of NCE.	**GIG1**
GIS-5.7.2	NCE shall be installed according to a defined plan and records of all installed NCE shall be maintained.	**GIG1**
GIS-5.7.3	NCE shall 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-5.7.4	NCE shall be physically secured from unauthorized access.	**GIG1**
GIS-5.7.5	GPE communications via NCE shall be logically secured from unauthorized access.	**GIG1**
GIS-5.7.6	NCE with limited onboard storage shall, if the audit log becomes full, disable all communication or offload logs to a dedicated log server.	**GIG1**
GIS-5.8	**Intrusion Detection System/Intrusion Prevention System (IDS/IPS)**	
GIS-5.8.1	An IDS/IPS shall 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" attack indicators and sever communications immediately if detected.	**GIG1**
GIS-5.8.2	The IDS/IPS shall 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-5.8.3	The IDS/IPS shall automatically disable any unauthorized or rogue devices connected to the GPE.	**GIG2**
GIS-5.8.4	The IDS/IPS shall maintain an access log which shall: 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-5.9	**Network Security Management**	
GIS-5.9.1	The Gaming Enterprise shall review and update policies and procedures to ensure the network is secure and threats and vulnerabilities are addressed accordingly.	**GIG1**
GIS-5.9.2	Networks shall 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-5.9.3	All network management functions shall authenticate all users on the network and encrypt all network management communications.	**GIG1**
GIS-5.9.4	The failure of any single item shall not result in a denial of service.	**GIG1**

GIS-5.9.5	All entry and exit points to the network shall be identified, managed, controlled, and monitored on a 24/7 basis.	**GIG2**
GIS-5.9.6	All network hubs, services and connection ports shall be secured to prevent unauthorized access to the network.	**GIG1**
GIS-5.9.7	Unused services and non-essential ports shall be either physically blocked or software disabled whenever possible.	**GIG1**
GIS-5.9.8	Stateless protocols, such as UDP (User Datagram Protocol), shall not be used for sensitive data without stateful transport. Note that although HTTP (Hypertext Transport Protocol) is technically stateless, if it runs on TCP (Transmission Control Protocol) which is stateful, this is allowed.	**GIG1**
GIS-5.9.9	All changes to network infrastructure shall be recorded in a 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-5.10	**Telecommuting and Mobile Computing**	
GIS-5.10.1	Telecommuting shall not be permitted except under circumstances where the security of the endpoint can be guaranteed.	**GIG1**
GIS-5.10.2	A formal policy shall be in place, and supporting security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.	**GIG1**
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 Gaming Enterprise for managing security controls does not exempt a Gaming Enterprise from the responsibly of ensuring that sensitive data is properly secured according to the applicable requirements.	**GIG1**
GIS-6.1.2	Clear policies and procedures shall be agreed between the Service Provider and the Gaming Enterprise for all security requirements, and responsibilities for operation, management and reporting shall be clearly defined and understood for each applicable requirement.	**GIG2**
GIS-6.1.3	Where sensitive data is shared with Service Providers, formal data processing agreements shall 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.	**GIG2**
GIS-6.2	**Service Provider Communications**	
GIS-6.2.1	The GPE shall be capable of securely communicating with Service Providers using encryption and strong authentication.	**GIG1**
GIS-6.2.2	All login events involving Service Providers shall be recorded in an audit file.	**GIG1**
GIS-6.2.3	Communication with Service Providers shall not interfere with or degrade normal GPE functions.	**GIG1**
GIS-6.2.4	Service Provider data shall not affect patron communications.	**GIG1**
GIS-6.2.5	Service Providers shall be on a segmented network separate from network segments hosting patron connections.	**GIG1**
GIS-6.2.6	Gaming shall be disabled on all network connections except for those within the GPE.	**GIG1**
GIS-6.2.7	The GPE shall not route data packets from Service Providers directly to the GPE and vice-versa.	**GIG1**
GIS-6.2.8	The GPE shall not act as IP routers between the GPE and Service Providers.	**GIG1**
GIS-6.2.9	Unauthorized Service Providers shall 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall be appropriate to the sensitivity of the data.	**GIG1**
GIS-7.2.3	The use of encryption methods shall be reviewed periodically to verify that the current encryption algorithms and key lengths are secure.	**GIG1**
GIS-7.2.4	The encryption method shall 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 shall be reviewed on a case-by-case basis.	**GIG1**
GIS-7.2.5	The management of encryption keys throughout their whole lifecycle shall follow defined processes established by the Gaming Enterprise.	**GIG1**
GIS-7.2.6	The Gaming Enterprise shall 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 shall 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 shall be established to monitor the expiration dates of encryption keys, where applicable.	**GIG1**
GIS-7.2.9	Procedures shall be defined for promptly revoking encryption keys in the event of compromise, loss, or unauthorized access.	**GIG1**
GIS-7.2.10	Procedures shall 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 shall 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 shall be established, documented, implemented, monitored, and reviewed.	**GIG1**
GIS-7.3.2	Configuration procedures for Critical System Components shall 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 shall be regularly assessed and, if appropriate, changes shall be made to improve the hardening.	**GIG2**
GIS-7.3.4	All default or standard configuration parameters shall be removed from all Critical System Components where a security risk is presented.	**GIG1**
GIS-7.3.5	Only one primary function shall 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 shall be implemented for any required services, protocols or daemons that are considered to be insecure.	**GIG1**
GIS-7.3.7	System security parameters shall be configured to prevent misuse.	**GIG1**

GIS-7.3.8	All unnecessary functionalities shall be removed, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	GIG1
GIS-7.4	**Generation and Storage of Logs**	
GIS-7.4.1	There shall be procedures established and documented to centrally monitor, manage, and respond to user activities, exceptions, faults, and adverse events.	GIG2
GIS-7.4.2	Security reports or logs shall be predefined and generated on each Critical System Component to monitor and rectify anomalies, flaws, and alerts.	GIG1
GIS-7.4.3	Security reports or logs shall be protected against tampering and unauthorized access.	GIG2
GIS-7.4.4	Security reports or logs shall be regularly reviewed as required by the Gaming Enterprise and/or the regulatory body.	GIG1
GIS-8	**Remote Access and Firewalls**	**GIG**
GIS-8.1	**Remote Access Security**	
GIS-8.1.1	Remote access security will 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 shall be appropriately secured and managed.	GIG1
GIS-8.1.3	The GPE shall have the ability to enable or disable remote access, and the default state shall be set to disabled	GIG1
GIS-8.1.4	Remote access shall accept only the remote connections permissible by the firewall application and system settings.	GIG1
GIS-8.1.5	Remote access shall 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
GIS-8.1.8	The GPE shall maintain an activity log depicting all remote access information. Remote access logs shall 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, shall 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 shall 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 shall 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 shall 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 shall be limited (e.g., network or system administrators only).	GIG1
GIS-8.2.7	The firewall shall reject all connections except those that have been specifically approved.	GIG1
GIS-8.2.8	The firewall shall 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 shall only allow remote access using encryption.	GIG1
GIS-8.2.10	The firewall shall be able to log audit information in a manner to preserve and secure the information from loss or alteration. This information includes the following: 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 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, shall be accounted for.	**GIG1**
GIS-9.1.2	Procedures shall exist for adding new assets and removing assets from service.	**GIG1**
GIS-9.1.3	A policy shall be included on the acceptable use of assets associated with the GPE.	**GIG1**
GIS-9.1.4	The designated owner of each asset shall: 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 shall 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 shall be correctly maintained, inspected, and serviced at regular intervals to ensure that it is free from defects or mechanisms that could interfere with its operation.	**GIG1**
GIS-9.1.8	Storage media shall 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 shall 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 shall be deleted when no longer required.	**GIG1**
GIS-9.1.11	Prior to disposal or re-use, assets containing storage media shall be checked to ensure that any licensed software, as well as sensitive data has been removed or securely overwritten.	**GIG1**
GIS-9.2	**Critical Asset Register (CAR)**	
GIS-9.2.1	A CAR shall 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 shall include hardware and software components and the inter-relationships and dependencies of the components.	**GIG1**
GIS-9.2.3	The following minimum items shall 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; 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 shall 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 shall 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 shall 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 shall be in place for all software components, source code, and binary controls.	**GIG1**
GIS-9.3.4	A CML shall 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 shall 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 shall cover managing releases through the outside party. This strategy may consider the severity of the issue. b. Otherwise, this strategy shall 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 shall be in place. Emergency changes shall be approved, tested, documented, and monitored.	**GIG1**
GIS-9.3.7	Procedures shall 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 shall be segregation of duties within the release process.	**GIG1**
GIS-9.3.9	Technical and user documentation shall be maintained, such as manuals and user guides, describing the systems in use and the operation, including hardware.	
GIS-9.3.10	Procedures shall 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 shall follow defined processes established by the Gaming Enterprise and/or regulatory body.	**GIG1**
GIS-9.4.2	The GPE shall 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 shall be established where applicable.	**GIG1**
GIS-9.4.4	The Gaming Enterprise shall 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 shall be integrated throughout the software development lifecycle, from initial requirements gathering to deployment and maintenance.	**GIG1**
GIS-9.4.6	The documented test methodology shall 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 shall be available and retained for the duration of its lifecycle.	**GIG1**
GIS-9.5	**Patch Management**	
GIS-9.5.1	The Gaming Enterprise shall have patch management policies agreed upon with the regulatory body, whether developed and supported by the Gaming Enterprise or by a Service Provider.	**GIG1**
GIS-9.5.2	The Gaming Enterprise shall 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 shall 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 and if authorized by the regulatory body, then patch testing shall be risk managed, either by isolating or removing the untested component from the network or applying the patch and testing after the fact.	**GIG1**

ANNEX I: SCORING THE RISKS

The following scoring system, based on the *Common Vulnerability Scoring System (CVSS)* and the *ISO/IEC 31010 Risk Management – Risk Assessment Techniques*, will be used for assessing the severity of security threats and vulnerabilities. It attempts to assign severity scores to threats and vulnerabilities, allowing prioritization of responses and resources according to the level of severity. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit.

Base Metrics: These metrics represent the most fundamental, immutable qualities intrinsic to vulnerability.

a. Access Vector: Measures how remote an attacker can be to attack a target.
b. Access Complexity: Measures the complexity of attack required to exploit the vulnerability once an attacker has gained access to the target system.
c. Authentication: Measures the number of times an attacker shall authenticate to the target system in order to exploit the vulnerability.
d. Integrity Impact: Measures the impact on integrity of a successful exploit of the vulnerability on the target system.
e. Confidentiality Impact: Measures the impact on confidentiality of a successful exploit of the vulnerability on the target system.
f. Availability Impact: Measures the impact on availability of a successful exploit of the vulnerability on the target system.

Temporal Metrics: These metrics represent the time dependent characteristics that evolve over the lifetime of vulnerability.

a. Exploitability: Measures how complex the process is to exploit the vulnerability in the target system.
b. Remediation Level: Measures the level of an available solution.
c. Report Confidence: Measures the degree of confidence in the existence of the threats and the credibility of its report.

Severity Rankings:

Severity	Score	Action Required
Critical	**9.0 – 10.0**	A critical vulnerability that shall be addressed immediately.
High	**7.0 – 8.9**	A vulnerability that presents a high risk and requires immediate attention and planning to remediate in the near future.
Medium	**4.0 – 6.9**	A vulnerability that presents a medium risk and requires investigation and planning to address during future system security improvements.
Low	**0.1 – 3.9**	A vulnerability that presents a low risk and should be addressed during routine system maintenance.
Info	**0.0**	An observation or finding worth noting for possible improvement to meet industry best practices.

ANNEX II: 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 Trail	A record showing who has accessed a system and what operations the user has performed 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
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 or retina patterns.
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 System Component	Any hardware, software, 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 which generate, transmit, or process random numbers used to determine the outcome of games and events.

Term	Descriptions
	• Components which store results or the current state of a patron’s game, wager, or available funds. • 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. • 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. • Corporate networks and systems that interface with the GPE and from which attackers could use to move laterally into the GPE, including corporate casinos’ networks and online operators’ corporate networks.
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.
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 Name Service (DNS)	The globally distributed internet database which (amongst other things) maps machine names to IP numbers and vice-versa.
Domain	A group of computers and devices on a network that are administered as a unit with common rules and procedures.
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 shall 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 Enterprises	Entities who oversee or are integrated to the functionality of a GPE, 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.

Term	Descriptions
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 an GPE or the sensitive data the GPE processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
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 shall 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.

Term	Descriptions
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.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
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.
"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.
Major Non-Conformity (MaNC)	A fundamental failing (systematic) has been identified that affects several controls and means that the overall security 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-conformance; or • Any non-conformance 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-conformance 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. Until resolved, such an issue will normally mean the Gaming Enterprise is not compliant with the GLI-GSF.
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.
Minor Non-Conformity (MiNC)	A 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. A course of action to remedy this should be provided with an appropriate timeline.
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, pattern or answers to challenge 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, facial or voice recognition).
Network Communication Equipment (NCE)	One or more devices that controls data communication in a system including, but not limited to, cables, switches, bridges, hubs, routers, wireless access points, and telephones.
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.

Term	Descriptions
Observation (OBS)	A policy is in place, but it is either not fully compliant with the GLI-GSF or the supporting evidence (or lack thereof) raised potential concerns. Any issues which are likely to become a non-conformance if not treated until the next audit are marked with this status.
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 patron. Examples include a legal name, date of birth, place of birth, social security number (or equivalent government identification number), driver's license number, passport number, residential address, phone number, email address, debit instrument number, credit card number, bank account number, 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. Making it more difficult for an attacker to obtain internal addresses and other details of the internal network.
Protocol	A set of rules and conventions that specifies information exchange between devices, through a network or other media.
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 shall have a valid Security Certificate.
Sensitive Data	Information that shall be handled in a secure manner, such as PII, gaming data, validation numbers, location data, authentication credentials, PINs, passwords, financial transactions, transfers of funds, patron tracking information, software packages, secure seeds and keys, RNG seeds, and any information which affects outcomes.
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.

Term	Descriptions
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.
Simple Network Management Protocol (SNMP)	A protocol used to configure, view, and in general, manage networked devices. Networked printers, switches, etc. often implement this protocol by default.
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 denial of service; the potential for a threat-source to successfully exploit a particular vulnerability; any potential danger to a network that someone or something may be able to identify as being vulnerable, and therefore seek to exploit.
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.
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).
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.
Virus Scanner	Software used to prevent, detect and remove computer viruses, including malware, worms and Trojan horses.
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

Term	Descriptions
	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.