BERMUDA GAMING COMMISSION (BGC)

BGC-6 CLIENT SERVER SYSTEMS STANDARDS

VERSION: 1.1

RELEASE DATE: OCTOBER 22, 2021

Table of Contents

Chapter 1: Introduction to Client Server Systems

1.1 Introduction

1.1.1 General Statement

Pursuant to section 199 of the Gaming Act 2014 ('the Act"), this technical standard prescribes criteria to be met for gaming machines.

The criteria are not exhaustive. All statutory requirements contained in the Gaming Act 2014 ("the Act") and the Gaming (Casino) Regulations 2018 ("the Regulations") shall be observed. This standard expressly applies for the purposes of the Regulations and section 93 of the Act. Approval shall be valid for a maximum term of 10 years and all applicable legislation and standards must be met on an ongoing basis.

These standards are of general application and seek to take account of the wide diversity of institutions which may be licensed under the Act. There may be need for revision of the standard from time to time. Material changes in the standards will be published generally by issuing a revised standard.

The integrity and accuracy of a Client Server System is highly dependent upon operational procedures, configurations, and the network infrastructure, and as such will require the development of internal processes and procedures to ensure that the system is configured and operated with the necessary level of security and control. Internal Controls will be established which prescribe the requirements for any system or component software and hardware, and their associated accounts.

1.2 Purpose of Equipment Standards

1.2.1 General Statement

The purpose of this equipment standard is as follows—

a) To eliminate subjective criteria in analyzing and certifying Client Server Systems.

b) To primarily test those criteria that impact the credibility and integrity of Client Server Systems from boththe revenue collection and patron's perspective.

c) To create a standard that will ensure bets on events are fair, secure, and able to be audited and operated correctly.

d) To recognize that the evaluation of internal control systems (such as Anti-Money Laundering,Financial and Business processes) employed by the casino operators of the Client Server System should not be incorporated into the laboratory testing of the standard but instead be included within the operational audit performed for local jurisdictions.

e) To construct a standard that can be easily revised to allow for new technology.

f) To construct a standard that does not specify any particular design, method, or algorithm. Theintent is to allow a wide range of methods to be used to conform to the standards, while at thesame time encourage new methods to be developed.

1.2.2 No Limitation of Technology

This document must not be read in such a way that limits the use of future technology. The Commission may review this standard and may make revisions as necessary to incorporate standards for new and related technology.

1.3 Interpretation of this Document

1.3.1 General Statement

This equipment standard applies to systems which support server-based gaming, server-supported gaming, or a hybrid of the two.

a) Server-supported gaming involves the combination of a server and gaming machines which together allow the transfer of the entire control programme and game content to the gaming machines for downloading control programmes and other software resources to the gaming machine on an intermittent basis. The gaming machines connected to the Client Server System can operate independently from the system once the downloading process has beencompleted unless the game is also server-based (hybrid).

b) Server-based gaming involves the combination of a server and gaming machines in which theentire or integral portion of game content resides on the server. This system works collectively in a fashion in which the gaming machine will not be capable of functioning when disconnected from the Client Server System. The server shall generate and transmit to the gaming machines control, configuration and information data, depending upon the actual implementation, examples are:

   i. Credit movement;

   ii. Random numbers;

   iii. Game result components, e.g., balls, cards or reel stop positions;

   iv. Actual game results; or

   v. Updates to the credit meter for winning games.

1.3.2 Software Suppliers and Casino Operators

The components of a Client Server System, although they may be constructed in a modular fashion, are designed to work seamlessly together. In addition, Client Server Systems may be developed to have configurable features; the final configuration of which depends on the options chosen by the casino operator. From a testing perspective, it might not be possible to test all of the configurable features of a Client Server System submitted by a software supplier in the absence of the final configuration chosen by the casino operator; however, the configuration that will be utilized in the production environment shall be communicated to the testing laboratory to facilitate creating a functionally equivalent test environment. Because of the integrated nature of a Client Server System, there are several requirements in this document which may apply to both casino operators and suppliers. In these cases, where testing is requested for a “white-label” version of the system, a specific configuration will be tested and reported.

1.4 Testing and Auditing

1.4.1 Laboratory Testing

The testing laboratory will test and certify the components of the Client Server System in accordance with the chapters of this equipment standard within a controlled test environment, as applicable. Any of these requirements which necessitate additional operational procedures to meet the intent of the requirement shall be documented within the evaluation reportand used to supplement the scope of the operational audit.

1.4.2 Operational Audit

In addition to the testing and certification of Client Server System components, the Commission may elect to require a periodic operational audit be conducted, using the recommended scope outlined within the appendices of the *BGC-3 Casino Gaming Electronic Monitoring System Standards.*

Chapter 2: Platform/System Requirements

2.1 Introduction

2.1.1 General Statement

If the Client Server System is comprised of multiple computer systems at various sites, the system as a whole and all communication between its components shall conform to the applicable technical requirements within this document.

2.2 System Clock Requirements

2.2.1 System Clock

The Client Server System shall maintain an internal clock that reflects the current date and time that shall be used to provide for the following—

a) Time stamping of all transactions and configuration changes;

b) Time stamping of significant events; and

c) Reference clock for reporting.

2.2.2 Time Synchronization

The Client Server System shall be equipped with a mechanism to ensure the time and dates between all components that comprise the system are synchronized and set correctly.

2.3 Control Programme Requirements

2.3.1 General Statement

In addition to the requirements contained within this section, the “Verification Procedures” sectionof this document shall also be met.

2.3.2 Control Programme Self-Verification

The Client Server System shall be capable of verifying that all critical control programme components contained on the system are authentic copies of the approved components of the system on demand using a method approved by the Commission. The critical control programmeauthentication mechanism shall—

a) 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;

b) Include all critical control programme components which may affect gaming operations, including but not limited to— executables, libraries, gaming or system configurations, operating system files, components that control required system reporting, and database elements that affect system operations; and

c) Provide an indication of the authentication failure if any critical control programme componentis determined to be invalid.

2.3.3 Control Programme Independent Verification

Each critical control programme component of the Client Server System shall have a method to be verified via an independent third-party verification procedure. The third-party verification process shall operate independently of any process or security software within the system. The testing laboratory, prior to system approval, shall evaluate the integrity check method.

2.4 System Functionality

2.4.1 Gaming Machine Functions

The purpose of this section is to ensure the functionalities of a conventional gaming machine are covered in a Client Server System environment by the gaming machine and/or Client Server System. It is understood that many software functions for a conventional gaming machine (e.g., Critical NV Memory, Machine Logs, Electronic Accounting and Occurrence Meters, Game HistoryRecall, etc.) may be covered by other

system components. In such cases these system components shall be evaluated against the applicable "Gaming Machine/Terminal Requirements" of the *BGC-1 Casino Gaming Machine Standards*.

2.4.2 Game Requirements

Games shall comply with the applicable "Game Requirements" of the *BGC-1 Casino Gaming Machine Standards*.

2.4.3 RNG Requirements

The Random Number Generator (RNG) shall comply with the applicable "Random Number Generator (RNG) Requirements" of the *BGC-1 Casino Gaming Machine Standards*.

2.4.4 Communication Requirements

If communication between the Client Server System and the gaming machine is lost, the software shall prevent display an appropriate error message. It is permissible for the software to detect this error when the device tries to communicate with the system. For server-based gaming, the software shall additionally prevent further gaming operations and provide a means, such as a hand pay, for players to cash out credits indicated on the credit meter at the time communication was lost.

2.5 System Components

2.5.1 Gaming Machine Requirements

Gaming machines used with a Client Server System may either be a display mechanism where the system performs all operations of the game (Thin Client) or contain its own logic function in conjunction with the Client Server System (Thick Client). Gaming machines shall comply with the applicable "Gaming Machine/Terminal Requirements" of the *BGC-1 Casino Gaming Machine Standards*.

NOTE: The hardware requirements may not apply to gaming machines that solely utilize unaltered commercial off-the-shelf (COTS) components, such as PCs or tablets.

For gaming machines that utilize modified off-the-shelf (MOTS) components, these requirements may apply only to the modifications made to the components.

2.5.2 Interface Element Requirements

Gaming machines may only communicate with external authorized components through a secure interface element, which does not allow such external connections to directly access the internal components, software or data of the gaming machines. The interface element shall comply with the applicable “Interface Element Requirements” of *BGC-3 Casino Gaming Electronic Monitoring System Standards*.

2.5.3 Software Security and Integrity

The Client Server System shall not be capable of altering any component on any connected gaming machine that would interrupt, or affect the functions, game outcome, or configurable options of a game in progress on any gaming machine connected to the Client Server System; provided however, that a Client Server System may suspend a game theme or disable a gaming machine at any time if there is a valid reason to do so.

2.6 Information to be Maintained

2.6.1 Data Retention and Time Stamping

The Client Server System shall be capable of maintaining and backing up all recorded data as discussed within this section in such manner as to be accessible upon request by the Commission for a period of not less than 7 years.

a) The system clock shall be used for all time stamping.

b) The system shall provide a mechanism to export the data for the purposes of data analysis and auditing/verification (e.g., CSV, XLS).

2.6.2 Download Activity Information

The information to be maintained and backed up by the Client Server System shall include for activity between the Client Server System and the gaming machine that involves the following, where supported;

a) Downloading of software to the gaming machine, including any programs it replaced;

b) Activation of previously downloaded software on the gaming machine, including any programsit replaced; and

c) Changes to the gaming machine configuration settings/configurations and what the changeswere

2.6.3 Significant Event Information

Significant event information to be maintained and backed up by the Client Server System shallinclude, as applicable—

d) Failed account access attempts, including IP Address;

e) Programme error or authentication mismatch;

f) Significant periods of unavailability of any critical component of the system (any length of time gaming is halted for all patrons, and/or transactions cannot be successfully completed for anyuser);

g) System voids, overrides, and corrections;

h) Changes to live data files occurring outside of normal programme and operating system execution;

i) Changes that are made to the download data library, including the addition, changing or deletion of software, where supported;

j) Changes to 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.);

k) Changes to date/time on master time server;

l) Changes to game theme parameters (e.g., game rules, payout schedules, rake percentage, paytables, etc.);

m) Irrecoverable loss of personal identification information (PII) and other sensitive information;

n) Any other activity requiring user intervention and occurring outside of the normal scope of system operation; and

o) Other significant or unusual events as deemed applicable by the Commission.

2.6.4 User Access Information

For each user account, the information to be maintained and backed up by the Client ServerSystem shall include—

a) Employee name and title or position;

b) User identification;

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) Group membership of user account (if applicable); and

i) The current status of the user account (e.g., active, inactive, closed, suspended, etc.).

2.7 Reporting Requirements

2.7.1 General Reporting Requirements

The Client Server System shall be capable of generating the information needed to compile financial reconciliation and variance reports as may be required by the legislation or by written direction of the Commission. In addition to meeting the requirementsin the section above for “Data Retention and Time Stamping”, the following requirements shall apply for required reports—

a) The system shall be able to provide the reporting information on demand, on a daily basis, and for other intervals required by the Commission (e.g., month-to-date (MTD), year-to-date (YTD), life-to-date (LTD), etc.).

b) Each required report shall contain—

   i. The casino operator’s name (or other identifier), the title of report, the selected intervaland the date/time the report was generated;

   ii. An indication of “No Activity” or similar message if no information appears for the periodspecified; and

iii. Labeled fields which can be clearly understood in accordance with their function.

NOTE: In addition to the reports outlined in this section, the Commission may also require other reports utilizing the information stored under the "Information to be Maintained" section of this document.

2.7.2 Change Reports

The Client Server System shall be able to provide the following information needed to compileone or more reports for a list of all software, paytable, and denomination changes:

a) Unique interface element/location identification number for the gaming machine;
b) Description of the change (additions, alterations, deletions, status changes, etc.)
c) The date and time of each change; and
d) Identification of the user performing the change

2.7.3 Download Data Library Reports

The Client Server System shall be able to provide the following information needed to compileone or more reports for software available in the download data library:

a) The software description,
b) The date and time the software was added to the library,
c) The date and time the game theme was last downloaded to a gaming machine,
d) Identification of the supplier, and
e) Identification of user who loaded the game theme into the library.

2.7.4 Significant Events and Alterations Reports

The Client Server System shall be able to provide the following information needed to compileone or more reports for each significant event or alteration, as applicable—

a) The date and time of the significant event or alteration;
b) Event/component identification;

c) Identification of user(s) who performed and/or authorised the significant event or alteration;

d) Reason/description of the significant event or alteration, including data or parameter altered;

e) Data or parameter value before alteration; and

f) Data or parameter value after alteration.

Chapter 3: Download Requirements

3.1 Introduction

3.1.1 General Statement

This chapter will outline the requirements of the Client Server System when downloading software, games and other configuration data to gaming machines, if the server provides the functionality of downloading control programmes and other software resources, whether for server-based gaming or server-supported gaming.

3.2 Download Data Library

3.2.1 General Statement

The Download Data Library refers to the formal storage of all approved data files that may be downloaded to gaming machines including software, peripheral firmware, configuration data, etc.

3.2.2 Update of Download Data Library

Where applicable, the Download Data Library shall only be written to, with secure access that is controlled by the Commission, in which case the operator will be able to access the Download Data Library, provided that this access does not permit adding new Download Data Files; or the Download Data Library shall only be written to using a method that is acceptable by the testing laboratory and the Commission.

3.3 Download of Gaming Machine Data Files and Software

3.3.1 General Statement

This section will outline the requirements of the Client Server System when downloading

software,games and other configuration data to gaming machines.

3.3.2 Update Conditions

Software shall not be activated, deactivated, added to, modified or removed from a gaming machine while an error or tilt condition, or hand pay lockup exists on the gaming machine, exceptas necessary to rectify the error condition.

3.3.3 Critical NV Memory Backup Prior to Downloads

Prior to any software being added or removed from a gaming machine, the accounting and security events data stored within the gaming machine's critical Non-Volatile (NV) memory, including metering, shall be stored on the Client Server System or communicated to the ElectronicMonitoring System when such a compatible system and protocol is supported.

3.3.4 Door Monitoring during Downloads

The gaming machine and/or the Downloadable Server shall have a method to monitor and report all external door access during a foreground program download and/or activation process to the on-line system when such a compatible system and protocol is supported.

NOTE: If the Downloadable Server does not have the ability to monitor the door access during the foreground program download and/or activation process, the testing laboratory's report shall indicate as such so that internal controls can be developed to ensure the security of the gaming machine'sexternal doors.

3.3.5 Forensic Analysis

It shall be possible to perform a forensic analysis of the game which may include viewing the game data at the Downloadable Server and/or being able to place the critical Non-Volatile (NV) memory back onto another gaming machine for examination purposes.

3.4 Conditions for Changing Active Software

3.4.1 General Statement

Active software consists of the following:

a) All the games currently available for play by the player on the gaming machine that do not first require additional software or a change in game configuration such as denomination, maximum wager, payback percentage, etc.; and

b) Any software in which a change will interrupt normal game play (e.g., operating system software and peripheral firmware).

3.4.2 Changing Active Software

The gaming machine shall be in the idle mode with no activity, no credits, no door open, and no error condition for at least two (2) minutes prior to the change in the active software unless the change is the direct result of a player request, or a qualifying event that is not an identifier, which may include, but is not limited to, the number of games played, or the cumulative amount wagered by a player during a gaming session as provided for in the rules of play.

3.5 Control of Gaming Machine Configurations

3.5.1 Paytable/Denomination Configuration Changes

Gaming machines may offer multiple paytables and/or denominations that can be configured viathe Downloadable Server, provided:

a) All paytables that are intended for use meet the “Software Requirements for Percentage Payout and Odds” required by the *BGC-1 Casino Gaming Machine Standards*.

b) The gaming machine and/or Client Server System maintains the “Paytable-Specific Meters” required by the *BGC-1 Casino Gaming Machine Standards* within critical NV memory for each of the paytables available;

c) The gaming machine maintains the “Electronic Accounting Meters” required by the *BGC-1 Casino Gaming Machine Standards* in local currency or the lowest

denomination available for the local currency;

d) The game is in an idle mode with no activity, no credits, no door open, and no error conditionwhen an update occurs; and

e) Any such change will not cause inaccurate crediting or payment.

3.5.2 Gaming Machine's Critical NV Memory Clear

The process of clearing the gaming machine's critical NV memory via the Downloadable Servershall utilize a secure methodology approved by the Commission.

Glossary of Key Terms

Act – The Gaming Act 2014.

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.

Authentication – Verifying the identity of a user, process, software package, or device, often asa prerequisite to allowing access to resources in a system.

Backup – A copy of files and programs made to facilitate recovery if necessary.

Casino – Any premises, or part of premises, within a designated site where persons may participate in one or more games approved by the Commission under section 91.

Casino Employee – An employee having functions in or in relation to a casino.

Casino Operator – A person who is the holder of a casino license.

Client Server System – The hardware, software, firmware, communications technology, other equipment, as well as casino operator procedures implemented in order to allow patron participation in server-based gaming, server-supported gaming, or a hybrid of the two. Both of which can be defined as the combination of servers, gaming machines and all interface elements that function collectively for the purpose of linking gaming machines with the Client Server System to perform a myriad of functions related to gaming, which may include, but are not limited to the downloading of software to the gaming machines, random number generation, and gaming configurations.

Commission – The Bermuda Gaming Commission (BGC) established under section 6 of the Act

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.

Critical Control Programme – A software programme that controls behaviors relative to any applicable equipment standard and/or regulatory requirement.

Data Integrity – The property that data is both accurate and consistent and has not been altered in an unauthorised manner in storage, during processing, and while in transit.

Encryption – The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorised people.

Encryption Key – A cryptographic key that has been encrypted in order to disguise the value ofthe underlying plaintext.

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 effectfor 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.

Internal Control Document – or “IC document” (for “internal control document”), in relation to acasino operator, has the meaning given in regulation 84.

Internal Control System – or “IC system” (for “internal control system”), in relation to a casino operator, has the meaning given in regulation 81.

Internal Controls – The controls, policies, rules, procedures and processes for the operations ofa casino.

Internet – An interconnected system of networks that connects computers around the world via TCP/IP.

IP Address, *Internet Protocol 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.

Key – A value used to control cryptographic operations, such as decryption, encryption, signaturegeneration or signature verification.

Key Data – Information relating to account balances, personal identification information (PII) andtransactional information.

Key Employee – A person in a key employee position.

Key Management – Activities involving the handling of cryptographic keys and other related security parameters (e.g., passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

Password – A string of characters (letters, numbers, and other symbols) used to authenticate anidentity or to verify access authorisation.

Printer – A Gaming Terminal peripheral that prints gaming tickets and/or wagering instruments.

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.

Regulations – The Gaming (Casino) Regulations 2018.

Remote Access – Any access from outside the system or system network including any access from other networks within the same site or casino.

RNG, *Random Number Generator* – A computational or physical device, algorithm, or system designed to produce numbers in a manner indistinguishable from random selection.

Secure Communication Protocol – A communication protocol that provides the appropriate confidentiality, authentication and content integrity protection.

Security Certificate – Information, often stored as a text file that is used by the Transport SocketLayer (TSL) Protocol to establish a secure connection. In order for an TSL connection to be created, both sides shall have a valid Security Certificate.

Security 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

Sensitive Information – Includes information such as PINs, key data, passwords, secure seedsand keys, and other data that shall be handled in a secure manner.

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”). In this case the “server” would be the Client Server System and the “clients” would bethe gaming machines.

Server-Based Gaming – Use of the combination of a server and gaming machines in which the entire or integral portion of game content resides on the server. This server works collectively in a fashion in which the gaming machine will not be capable of functioning when disconnected fromthe Client Server System. The server shall generate and transmit to the gaming machines control, configuration and information data, depending upon the actual implementation.

Server-Supported Gaming – Use of the combination of a server and gaming machines which together allow the transfer of the entire control programme and game content to

the gaming machines for downloading control programmes and other software resources to the gaming machine on an intermittent basis. The gaming machines connected to the Client Server System can operate independently from the system once the downloading process has been completed unless the game is also server-based (hybrid).

Source Code – A text listing of commands to be compiled or assembled into an executable computer program.

Supervisory Employee – A member of staff in a supervisory employee position.

System Administrator – The individual(s) responsible for maintaining the stable operation of the Client Server System (including software and hardware infrastructure and application software).

TCP/IP, *Transmission Control Protocol/Internet Protocol* – The suite of communications protocols used to connect hosts on the Internet.

Testing Laboratory– means a laboratory contracted by the Commission for the purposes of determining the suitability of gaming equipment.

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 unauthorised access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a system vulnerability.

Time Stamp – A record of the current value of the Client Server System date and time which is added to a message at the time the message is created.

Touch Screen – A video display device that also acts as a user input device by using electrical touch point locations on the display screen.

Unauthorised Access – A person gains logical or physical access without permission to a network, system, application, data, or other resource.

User Interface – An interface application or programme through which the user views and/or interacts with the Gaming Software to communicate their actions to the Client Server System.

Version Control – The method by which an evolving approved Client Server System is verified to be operating in an approved state.

Voucher – A wagering instrument which can be redeemed for cash or used to subsequently redeem for credits.

VPN, *Virtual Private Network* – A logical network that is established over an existing physical network and which typically does not include every node present on the physical network.

Vulnerability – Software, hardware, or other weaknesses in a network or system that can providea “door” to introducing a threat.

Wagering Instrument – A printed or virtual representative of value, other than a chip or token and includes coupons and vouchers. A virtual wagering instrument is an electronic tokenexchanged between a patron's mobile device and the Gaming Terminal which is used for credit insertion and redemption.