Tasmanian Liquor and Gaming Commission

Gaming Machine Electronic Monitoring System Technical Standards

1 July 2023

Gaming Machine Electronic Monitoring System Technical Standards

An electronic copy of these Standards is available at
https://www.treasury.tas.gov.au/liquor-and-gaming/gambling/regulatory-requirements

For further information please contact:

Liquor and Gaming Branch
Department of Treasury and Finance
GPO Box 147
HOBART TAS 7001
(03) 6166 4040 or gaming@treasury.tas.gov.au

Contents

Preliminary

These Gaming Machine Electronic Monitoring System Technical Standards are made in accordance with section section 112PA of the *Gaming Control Act 1993* (the Act) and apply to the conduct of gaming and gaming activities. A prescribed licence holder and its employees must adhere to and enforce these Standards. Failure to comply may result in disciplinary action against the prescribed licence holder.

A term used in these Standards has the same meaning as the same term used in the Act. A reference in these Standards to 'wagering' means a 'gaming activity' under the Act. For the avoidance of doubt, a reference to an 'employee of the licence holder' includes the licence holder's agent or, where the licence holder is a natural person, itself.

These Standards are in addition to the conditions imposed on each licence by the Tasmanian Liquor and Gaming Commission and any other requirement under the Act.

Gaming Machine Electronic Monitoring System Technical Standards

1. Introduction

1.1 Authority

1.1.1. These standards are authorised and issued as standards by the Tasmanian Liquor and Gaming Commission (the Commission) under section 112PA of the *Gaming Control Act 1993* (the Act).

1.1.2. The Act requires that all gaming machines operating in licensed venues must be connected to an approved electronic monitoring system (EMS).

1.1.3. In these standards, the term monitor refers to either a casino licensee in the case of a casino licensed to operate gaming machines or a licensed monitoring operator in the case of a person licensed to monitor gaming machines in hotels or licensed clubs in Tasmania.

1.1.4. An EMS used by a monitor must be approved by the Commission in accordance with the Act.

1.1.5. The Act requires that a monitor must have a system of internal controls and administrative and accounting procedures approved by the Commission.

1.1.6. The requirements specified in these standards are supplementary to, and do not take the place of, any of the requirements of the Act or any regulations made under the Act.

1.2 Objective

1.2.1. The objective of these standards is to require that the EMS operated by a monitor in Tasmania, is designed to enable:

a) The integrity of the hardware, software, interfaces, and networks used to connect components of the EMS and gaming machines;

b) The security and integrity of transactions between gaming machines and the EMS;

c) The accurate monitoring, recording, reporting, and secure storage of information gathered from connected gaming machines;

d) Only approved gaming machines and games are available for play in licensed venues in Tasmania;

e) The correct calculation of gross profit;

f) The correct awarding of player entitlements;

g) An efficient process and capability to approve games and gaming equipment, and to manage and respond to support or service requests from the Commission, the Liquor and Gaming Branch, and licensed venue operators;

h) Collection of data and information that may be used for research purposes;

i) Efficient processes and capability for the configuration management of gaming machines, games, and jackpot arrangements without undue burden on the Commission, and licensed venue operators;

j) The capability of being modified or adapted to incorporate new technologies over the term of a licence, such as new gaming machine interface protocols, new gaming machine types and system security measures; and

k) Modification to support future harm minimisation requirements without the need for significant redesign of the EMS.

1.2.2. These standards do not set out the content of internal controls or administrative and accounting procedures required of a monitor. However, it is expected that such controls and procedures will address requirements outlined in these standards.

1.2.3. A monitor is required under the Act to receive approval from the Commission for its proposed system of internal controls and administrative and accounting procedures.

1.2.4. It is not the intent of these standards to unreasonably restrain the design, innovation, and application of technologies of an EMS.

1.2.5. These standards set out EMS requirements but does not seek to prescribe system implementation methods or use of specific technology to enable compliance with these standards.

1.3 Scope and Purpose

1.3.1. These standards describe the Commission's minimum technical and system requirements for an electronic monitoring system to be used by a monitor in Tasmania.

1.3.2. These standards must be used to evaluate a monitor's proposed EMS for compliance with the Commission's requirements, or to evaluate changes to previously approved versions of their EMS for approval.

1.3.3. These standards will be used by an ATF to independently test an EMS, including any changes, and certify EMS compliance with these standards.

1.3.4. These standards will be used by the Commission to evaluate compliance by a monitor with the requirements of their licence, and to evaluate changes to previously approved versions of an EMS, in accordance with the Act.

1.3.5. Compliance with these standards does not exempt a monitor or supplier from compliance with other laws (e.g. laws relating to privacy, consumer protection, prohibited content, copyright, electrical safety and electronic cash transactions).

1.3.6. Future updates to these standards do not automatically require modification to an EMS approved and operating at that time, unless specifically required by the Commission.

1.4 Gaming Machine Communication Protocols

1.4.1. These standards, and the Commission, does not seek to mandate the use of any specific gaming machine communication protocol.

1.4.2. Prior to the commencement of monitoring activities, a monitor must satisfy the Commission that an EMS is capable of interfacing and communicating with all variants of gaming machine protocols operating in Tasmania.

1.4.3. The design of an EMS is expected to cater for the support of additional gaming machine communication protocols without major disruption or change to EMS components or software.

1.4.4. The Commission reserves the right to direct an EMS to support one or more specific gaming machine communications protocols. However, the timing for introduction of future protocol support would be negotiated with the monitor.

1.4.5. An EMS must at all times operate in accordance with gaming machine communications protocol specifications operated by gaming machines and linked jackpot equipment connected to the EMS.

1.5 Interpretation

1.5.1. Any comments or questions relating to understanding or interpretation of any aspect of these standards should be referred to the Liquor and Gaming Branch for clarification.

1.6 Potential for Dispensations

1.6.1. Matters arising from the testing of an EMS that have not been addressed in these standards will be resolved at the sole discretion of the Commission, as part of the approval process.

1.6.2. At the sole discretion of the Commission, components of an EMS which do not fully comply with all the requirements of these standards, may be considered for approval, provided the EMS operates in a manner that is suitable in respect of fairness, security, integrity, and consumer protection.

1.7 Equipment Statutory Testing and Certification

1.7.1. A monitor must only operate EMS equipment that is compliant with prevailing statutory and applicable EMI, EMC, electrostatic interference, and safety standards administered by relevant regulatory bodies through international and/or Australia/New Zealand or local standards.

1.8 Associated Documentation

1.8.1. Monitors should familiarise themselves with the following documents and their respective impact on the design and functionality of their EMS:

a) *Gaming Control Act 1993*
b) Australian/New Zealand Gaming Machine National Standard
c) Tasmanian Appendix to the Australian/New Zealand Gaming Machine National Standard
d) QCOM Gaming Machine Communication Protocol and other QCOM Technical Standards
e) TLGC Card Based Gaming Systems Technical Standards
f) TLGC Linked Jackpot Equipment Technical Standards
g) TLGC Fully Automated Table Game Technical Standards
h) TLGC Responsible Gambling Mandatory Code of Practice
i) *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
j) *Privacy Act 1988*
k) ISO/IEC 27000 Information Security Management System series
l) ISO/IEC 9000 Quality Management System series
m) Australian Government Information Security Manual

1.9 Copyright

1.9.1. These standards are the property of the State of Tasmania (Department of Treasury and Finance).

1.9.2. Copying, making extracts or use of these standards, without prior permissions is prohibited.

2. General Requirements

2.1 Functionality

2.1.1. An EMS must have the following functionality:

a) Integrity management of gaming machines, including:
   i. authentication of gaming machine software
   ii. verification of game parameter settings
   iii. managing venue operating hours for gaming machines

b) Monitoring of gaming machines and game play, including:
   i. collection of events related to gaming machines and game play
   ii. collection of gaming machine meters
   iii. collection of gaming machine and communications security/integrity events

c) Monitoring of external jackpot arrangements for gaming machines, including:
   i. management of approved jackpot configurations
   ii. authentication of software associated with linked jackpot equipment connected to gaming machines
   iii. monitoring of events related to linked jackpot equipment operations
   iv. collection of linked jackpot arrangement meters
   v. jackpot pool reconciliation

d) Control of gaming machine play, including:
   i. the ability to enable and disable a gaming machine for play
   ii. communications via structured communication protocols
   iii. facilitation and authorisation of hand-pays
   iv. implementation of venue operating hours

e) Accounting and reporting, including:
   i. calculation of gross profit by venue
   ii. production of standard reports required by the Commission
   iii. production of reports and data for venue operators, including gross profit, estimated taxation and community support levy amounts to assist in venue accounting functions
   iv. production of reports related to usage of EGM consumer protection measures (where available)
   v. the ability to produce reports and data, based on ad-hoc requests

f) Facilitation of services (directly or indirectly), including:
   i. card based gaming
   ii. player loyalty
   iii. player pre-commitment and consumer protection services

iv. connection with licensed venue operator owned equipment used for in-venue gaming machine reporting or other data reporting.

2.1.2. A monitor must implement and operate an EMS in a service management framework, supported by policies, standards and procedures covering:

a) A service support and help desk function, incorporating:
   i. incident management
   ii. problem management
   iii. configuration management
   iv. change management
   v. release management

b) A service delivery function, incorporating:
   i. availability management
   ii. capacity management
   iii. service level management
   iv. service continuity management

c) Security management, including:
   i. the establishment and management of an information security management system (ISMS) that meet ISO/IEC 27001:2013 or equivalent

d) Data and cyber security, including:
   i. data governance
   ii. cyber security as set out in the Australian Government Information Security Manual
   iii. anti-virus management of the EMS

e) Quality management system, including:
   i. the establishment and management of an information security management system that meets ISO/IEC 9000 or equivalent

f) ICT Infrastructure management (hardware and software), including:
   i. the design, deployment, and operational management of ICT equipment and software in the provision of the EMS, as approved by the Commission

g) Application management, including:
   i. the ongoing management of the EMS including, but not limited to, designing, testing, operating, improving and support

2.1.3. An EMS must be configured to only permit the live operation of approved gaming machines, games, jackpot configurations, and linked jackpot equipment.

2.1.4. An EMS must provide a secure connection with all gaming machines and other relevant gaming equipment operating in conjunction with gaming machine games.

2.1.5. An EMS must have the capacity to provide a range of different access levels for its users based on specific security requirements relevant to EMS user duties.

2.1.6. An EMS must not permit the operation of games in the event of a loss of communication to the EMS, where the loss of communication is able to adversely impact the EMS's ability to control, record, and monitor significant game and jackpot events.

2.2 Design Capacity

2.2.1. An EMS must be designed and implemented to provide continuous (24 hours per day, seven days per week) monitoring of gaming machines and linked jackpot equipment.

2.2.2. All components of an EMS must comply with the requirements of these standards.

2.2.3. All EMS components must be approved by the Commission.

2.2.4. An EMS must be flexible and scalable to cater for changes in requirements and standards (as determined from time to time by the Commission), new and emerging technology and to cater for growth in transactions and expansion of gaming products and services.

EMS Software and Central EMS Host

2.2.5. EMS software, a central EMS host and a wide area network (WAN) must be designed and configured to connect to, and manage data transmission between, the central site and licensed venues operating gaming machines in Tasmania (where applicable).

2.2.6. It must be possible to increase the number of licensed venues connected to the central EMS host (where applicable) without a change in computing and storage resources, or design of the EMS software, central EMS host, and WAN, and without detriment to the EMS operational performance.

2.2.7. EMS software and a central EMS host must be designed and configured to receive financial data records from all licensed venues (where applicable) within one hour from the EMS end-of-day time.

2.2.8. A monitor must provide physical and electronic access to the central EMS host facilities and EMS software to a Liquor and Gaming Branch Inspector on request.

Venue EMS Host

2.2.9. EMS software and a venue EMS host must be designed to:

a) Connect and manage data transmission between the venue EMS host and at least 60 simultaneously operating gaming machines;

b) Collect and manage at least 12 multi-game meter sets for each connected gaming machine;

c) Manage and operate at least four linked jackpot arrangements, each with at least eight jackpot levels;

d) Communicate with gaming machines approved and operating with different gaming machine communication protocols (Note: protocol converters must be approved for use by the Commission);

e) Initiate software set authentications for all connected gaming machines and linked jackpot equipment;

f) Collect and report gaming machine meters and events and jackpot events, as set out in these standards; and

g) Facilitate local area and wide area cryptographic data security requirements, as set out in these standards.

2.2.10. In the event of loss of communications between the central EMS host and a venue EMS host, the venue EMS host must disable all gaming machines and linked jackpot arrangements in that venue if communications to the central EMS host are not restored to an operational state at the expiration of <down_time_permitted>.

Disaster Recovery Capability

2.2.11. The EMS must be designed and operated with an integrated disaster recovery capability including redundant central EMS host infrastructure, including databases, installed and operating from a separate physical location that can be switched from primary to secondary mode without loss of data or events.

3. EMS Hardware

3.1 Capacity and Performance

3.1.1. An EMS must be configured, and operated, with sufficient capacity (e.g. number of CPUs, memory, storage, and network bandwidth) to meet the requirements of these standards and for the monitoring of all gaming machines licensed venues in Tasmania (where applicable).

3.1.2. The architecture of an EMS must be designed such that under normal operating conditions, no single point of failure would interrupt the operation of the EMS.

3.2 Central Site and Disaster Recovery Site EMS Environment

Secure environment

3.2.1. The central components of a central EMS and disaster recovery EMS must be located in secure areas (e.g. computer room) where only authorised personnel can enter, which incorporate an electronic locking system that provides monitoring information on the entry and exit of all personnel.

3.2.2. Access to any EMS computer room must be secured and controlled.

3.2.3. An EMS computer room must include CCTV monitoring and recording of access into and out of the room, as well as coverage within the room to clearly show movement of people and access to equipment at any location in the room.

3.2.4. Procedures must be established and maintained to allow only authorised personnel to access an EMS computer room.

3.2.5. There must be a detection system that records an audit log entry which must provide an alert when unauthorised entry to the computer room is attempted.

Environmental Monitoring System

3.2.6. All machinery, equipment, and computer systems within the central components of an EMS computer room environment must be supported by an environmental monitoring system.

3.2.7. The environmental monitoring system must be able to check the parameters of the environment that are required for the safe and continual working operation of the EMS and to automatically alert if these conditions are not met.

Power Supply

3.2.8. A monitor must have at least one uninterruptible power supply (UPS), and at least one stand-by generator in place, for all machinery, equipment, and computer systems within or contributing to the central components of an EMS computer room(s) environment.

3.2.9. A monitor must establish and maintain policies, standards, and procedures to enable computer systems to be shut down in a controlled and auditable manner without the loss of data, and must include provision should a UPS or stand-by generator fail.

3.2.10. Mains power interruptions to the central components of an EMS must not impact the integrity of the EMS or its components.

Uninterruptible Power Supply (UPS)

3.2.11. The computer, security, and telecommunication systems within or contributing to the central components of an EMS must be protected against power fluctuations and temporary loss, by installation of a UPS or other such device.

3.2.12. A UPS must provide a sufficient power supply to support the continued operation of central components of an EMS for up to two hours on full load until a stand-by generator is started, or to enable the systems to be shut down in an orderly manner without the loss of data, should the generators fail.

3.2.13. All machinery, equipment and computer systems situated in the central components of an EMS computer room must be earthed via the UPS.

Stand-by Generator

3.2.14. The central components of an EMS must be protected against loss of power by the installation and maintenance of a generator. The generator must have the capacity to support computer systems, air conditioning, security system, telecommunication equipment, computer terminals, environmental monitoring system and sufficient lighting for normal operation of the central components of the EMS and facilities for a period of not less than 24 hours.

Emergency Lighting

3.2.15. The central components of an EMS computer room must have an emergency lighting system that automatically activates when mains power is lost. If this operates from the UPS, there must be sufficient capacity in the UPS to cater for the lights, plus computers and air conditioning.

Disaster Recovery Testing

3.2.16. A monitor must test a central site UPS, stand-by generator, emergency lighting and any related systems or procedures at least every three months. Records of this testing must be provided to a Liquor and Gaming Branch Inspector upon request.

3.2.17. A monitor must test its procedures and facilities and log outcomes in a logbook or equivalent. The monitor must provide this information for inspection by a Liquor and Gaming Branch Inspector upon request.

Cloud Computing Environment for Central EMS Hardware

3.2.18. A monitor may apply to the Commission to utilise a cloud computing environment as an alternative to EMS hardware owned or operated by the monitor.

3.2.19. Applications to utilise a cloud computing environment must include:

a) A description of the cloud service model (e.g. software as a service, platform as a service, or infrastructure as a service);

b) A description of the of the proposed cloud model (e.g. private cloud, community cloud, public cloud, hybrid cloud) and sufficient details of the cloud owner and operator to support the application;

c) Details of which applications of the EMS are intended to operate in a cloud environment;

d) Details of where EMS applications, databases and other records are stored;

e) Details of a risk assessment conducted by the monitor into the cloud service provider and the proposed cloud environment;

f) Details of how disaster recovery and physical separation of EMS host infrastructure will be implemented;

g) How the requirements for security, environmental monitoring, power supply, UPS and standby generator outlined in this section are met; and

h) Any other information requested by the Commission in consideration of the application.

3.2.20. A monitor must comply with the requirements of the Act in relation to Commission approval for certain contract arrangements and exemptions for storage of records.

3.2.21. Any contract between a monitor and a cloud or third party computing provider must include the following requirements:

a) Access to all gaming equipment and records stored on third party infrastructure is restricted to the monitor;

b) Gaming equipment and records are managed and maintained in accordance with these standards;

c) Gaming equipment and records are only operated from third party infrastructure locations within Australia;

d) The monitor maintains full control and ownership of all gaming equipment and gaming records stored on third party infrastructure; and

e) In the event the contract is terminated, suitable controls must be in place with the third party storage provider to enable normal access and recovery of the monitor's gaming equipment and gaming records.

3.3 Venue-based EMS Hardware

3.3.1. Venue-based EMS hardware components, such as a venue EMS host (sometimes called a site controller), network switch, and wide area (internet) network terminating units, must be securely located away from public areas.

3.3.2. All models and configuration of venue-based EMS hardware components must be approved by the Commission and must be documented in the EMS baseline document approved by the Commission.

3.3.3. All venue-based EMS hardware components, of any one hardware revision level, must be identical across all licensed venues (where applicable) unless otherwise approved by the Commission (e.g. a venue EMS host of one hardware revision level must not have different internal wiring, components, firmware, and circuit boards from another venue EMS host of the same model and revision number).

3.4 EMS Hardware in Gaming Machines

3.4.1. Where an EMS requires hardware to be installed in, or connected to, gaming machines, other than local area network cabling (e.g. interface devices or protocol converters), such hardware must be approved for use by the Commission.

3.4.2. EMS hardware installed in, or connected to, a gaming machine must be securely housed within a locked area of the gaming machine.

4. Minimum EMS Functions

4.1 Gaming Approvals Databases

General

4.1.1. A monitor must provide secure and auditable on-line facilities, in addition to an approval database(s), that support the following services:

a) An on-line service that provides a capacity for manufacturers and suppliers to transmit new gaming machine game and gaming equipment submissions intended for evaluation and approval in Tasmania;

b) An on-line service that provides the Liquor and Gaming Branch access to transmitted gaming machine game and gaming equipment submissions for the purposes of conducting evaluations;

c) An on-line service that enables the Liquor and Gaming Branch to electronically issue Commission approval notices for gaming machine games and gaming equipment;

d) An on-line service that enables the Liquor and Gaming Branch to electronically issue Commission withdrawal notices for gaming machine games and gaming equipment;

e) An on-line service that enables the Liquor and Gaming Branch to download and obtain gaming machine and equipment approval information from the EMS database(s).

f) An on-line service that provides licensed venues (where applicable) with a capacity to submit gaming machine game and gaming equipment change requests.

4.1.2. An EMS must maintain one or more databases to record accurate details of licensed venues (where applicable), gaming machine manufacturers, gaming machines, game operating systems, games and linked jackpot arrangements approved for gaming in Tasmania, which are required to be monitored by the monitor.

4.1.3. EMS databases must retain details of all gaming equipment approvals issued by the Commission along with historical data to enable determination of applicable approval period(s).

4.1.4. An EMS must update and maintain all gaming machine game and gaming equipment approvals required by these standards in a timely and efficient manner.

4.1.5. An EMS gaming approvals database and EMS software must not allow withdrawn or unapproved games to be configured for operation, or operate in a licensed venue (where applicable).

4.1.6. A monitor must receive approval from the Commission for gaming machine or game software versions, and linked jackpot arrangements before they are loaded into the EMS gaming approvals database.

4.1.7. A monitor must be able to receive additional licencing and approvals data from the Liquor and Gaming Branch for entry into EMS gaming approval databases. Information must be able to be transmitted electronically to the EMS from the Liquor and Gaming Branch's computer systems.

4.1.8. Current and historical records must be accessible for a period of at least seven years.

Management of Gaming Approvals databases

4.1.9. An EMS must contain functionality for authorised users to create, edit and view records in gaming approval databases.

4.1.10. Gaming approval databases must be designed and configured in a manner that reduces, or eliminates the need for replicated data storage, or reprocessing of information received from the Liquor and Gaming Branch as part of approval applications.

4.1.11. All access to, creation and editing of gaming approval database records must be logged and include sufficient information to inform an auditor of the nature of such access or data editing, including details of the user, date, time, terminal identification, data created and/or edited, and a reference identifier required to be input by the user at the time of access (such as a Commission approval number or a Liquor and Gaming Branch authorised job number).

4.1.12. The approval process to grant an EMS user authority to access functions to manage gaming approvals databases must include authorisation from the Liquor and Gaming Branch and user rights that allow database creation or editing of records which must be securely logged for later access by auditors.

Licensed Venue details database records

4.1.13. Records must accurately identify each licensed venue (where applicable), including venue name, Commission issued licence number, venue type (casino, hotel or licensed club), address and key contact(s) authorised to represent the licensee.

4.1.14. Records must accurately identify the maximum permitted number of gaming machines in each licensed venue (where applicable), as well as the up-to-date number of approved gaming machines.

4.1.15. An EMS must maintain up-to-date records of the approved gaming hours for each day of the week for each licensed venue (where applicable).

Approved Gaming Machine Manufacturer Database Records

4.1.16. Records must accurately identify each approved gaming machine manufacturer, including a short form manufacturer ID (MID) and full descriptive name.

Approved Gaming Machine Models Database Records

4.1.17. Records must accurately identify all gaming machine models approved for use in Tasmania, including MID, serial number, model name, and model type.

Approved Game Operating System Versions Database Records

4.1.18. Records must accurately identify all approved versions of gaming machine operating software (sometimes called base or shell) for each gaming machine model for each manufacturer.

4.1.19. Accurate details of the gaming machine interface protocol implemented in each gaming machine operating system version must be maintained, including the protocol short form name, and the full version number (e.g. QCOM as a protocol short form name, and 1.6.6 as the full version number).

4.1.20. Records must accurately identify the algorithm/process required for periodic authentication of each game operating system and games/software sets approved for operation with it.

Approved Games and Variations Database Records

4.1.21. Records must accurately identify each game/variation combination approved for use in gaming machines in Tasmania.

4.1.22. Records must include key defining information contained in the game/variation approval issued by the Commission, including game name, game program number, base/shell

number, software set number, lines/ways combinations, MID, PID ID, jurisdiction ID, theoretical RTP percentage, maximum jackpot prize, and maximum bet.

4.1.23. Records must include the game credit denomination, or in the case of multi-denomination games, all approved denominations must be recorded.

4.1.24. If a game/variation is contained in a multi-game software set, records must identify the software set version number and all games within that set.

4.1.25. If a game operates with standalone progressive jackpots, the records must include the number of jackpot levels, and for each level, its ID/name, theoretical RTP%, start-out amount, maximum jackpot prize, and progressive increment rate.

4.1.26. If the game operates in an external linked progressive jackpot arrangement, the records must include the external linked jackpot arrangement name/ID, the number of jackpot levels, and the name/ID for each level.

Approved Linked Jackpot Arrangements Database Records

4.1.27. Records must accurately identify all linked jackpot arrangements approved for use in licensed venues in Tasmania.

4.1.28. Each linked jackpot arrangement must be identified by its approval number issued by the Commission.

4.1.29. Records for each approved linked jackpot arrangement must accurately identify the jackpot category, such as linked progressive or random/mystery.

4.1.30. For each approved linked jackpot arrangement, records must include an identifying short form name of the link, the manufacturer and game variations approved to patriciate in the link, and the number of jackpot levels.

4.1.31. Defining parameters of each level of each linked jackpot arrangement must be accurately recorded, including approval number, link short form name, level number, level name, start-out (or reset) value, pool increment rate, maximum pool value and treatment of overflow pools (if any).

Approved EMS software Database Records

4.1.32. An EMS must maintain accurate records of all versions of EMS software operating in EMS hardware components.

4.1.33. Records must accurately identify details of the hardware device that the software set is applicable to, software set version number, and Commission approval date.

4.1.34. Records must accurately identify the date each software set was installed in an EMS component in the central EMS host and at each licensed venue (where applicable).

4.1.35. Historical records must be maintained for any previous approved software set installation in any EMS component for at least seven years.

4.2 Licensed Venue Gaming Configuration Management

4.2.1. An EMS must maintain accurate and up-to-date records of the approved gaming configuration in each licensed venue (where applicable), including total number of gaming machines, identification of each gaming machine and game(s), linked jackpot arrangements operating in the licensed venue and licensed gaming hours of that licensed venue.

4.2.2. For each gaming machine location in a licensed venue, the EMS must accurately record a floor location number, as well as the gaming machine serial number.

4.2.3. An EMS must accurately record game(s) configurations for each gaming machine in a licensed venue.

4.2.4. For each linked jackpot arrangement configured in a licensed venue, an EMS must accurately record the floor location and serial number for all contributing EGMs.

4.2.5. An EMS must accurately record the commencement date, and subsequent retirement date, for every unique combination of gaming machine, game operating system, game(s) and game variation, and participation in any linked jackpot arrangement approved for operation, for all floor locations in a licensed venue.

4.2.6. Historical records for previous approved configurations at all floor locations in a licensed venue must be maintained by an EMS for at least seven years.

4.2.7. An EMS must facilitate an online electronic mechanism for venue operators or licensed service providers to submit proposed changes to the gaming configuration at any floor location in a licensed venue. Such a mechanism must facilitate "pre-loaded" configurations (e.g. ahead of a planned commencement date) that can be compiled and submitted effectively, enable configuration pre-checking by a monitor, and upgrade to live status without reliance on manual processes.

4.2.8. An EMS must facilitate an online electronic process for the management of approved gaming operating hours for each licensed venue.

4.2.9. An EMS must facilitate an online electronic process to enable the creation of new licensed venue records and the retirement of existing licensed venues (based on records from the Commission).

4.3 Authentication

Software Set Authentication

4.3.1. An EMS must have the capacity to enforce compulsory authentication of all gaming machine software and venue-based EMS component software (including the venue EMS host) via a validation method approved by the Commission.

4.3.2. A validation method must not use static hashing techniques to perform software authentication.

4.3.3. The following validation methods must be used:

a) A short term (daily) seed to calculate a software set hash result;

b) A randomly selected seed from a large pool of seeds to calculate a software set hash result; or

c) Another software authentication method that provides equivalent levels of authentication to those stated above.

4.3.4. An EMS must include a process to validate software set authentication results against corresponding approvals issued by the Commission.

4.3.5. Failure of authentication of any individual instance of a software set must be reported to the Commission as a significant security event by the EMS and that gaming machine or EMS component must not be enabled.

4.3.6. Software set authentication of gaming machine software and venue-based EMS component software must be capable of being initiated on a scheduled basis, in response to pre-set events and by an authorised operator request.

Gaming Machine and Game Configuration

4.3.7. An EMS must validate a gaming machine and its game parameters against approved values stored in the EMS gaming approvals database (e.g. configured EGM RTP, minimum RTP, maximum bet, lines/ways combination, and participation in jackpot arrangements (SAP or linked)).

4.3.8. Failure of an EMS to confirm a gaming machine or games are configured with approved parameter settings must be reported as a significant security event to the Commission and that gaming machine must not be enabled.

4.4 Control

General

4.4.1. An EMS must be able to control the availability of gaming machine operations in a licensed venue by enabling/disabling gaming machines or venue-based EMS components.

Operation of Authenticated Devices Only

4.4.2. An EMS must not permit any venue-based EMS equipment to operate until all software sets on that equipment have completed an authentication test initiated by a higher-order EMS component (e.g. closer to the central EMS host), or the central EMS host, and the results confirm that the approved software set version is installed on that device.

4.4.3. An EMS must not permit a gaming machine to be enabled for play until all software sets on that gaming machine have completed EMS initiated authentication tests, and the results have been verified by the EMS confirming that the approved game software set version has been installed on that gaming machine.

Gaming Machine or Game Parameters

4.4.4. An EMS must be able to set all gaming machine and game parameters supported by the gaming machine communication protocol operating in any gaming machine.

4.4.5. A monitor must implement any specific elements or function available within a gaming machine communication protocol via the EMS if directed to do so by the Commission under the Act, within the permitted timeframe.

4.4.6. An EMS must enforce all limits and controls on gaming machines and games required by the Act, regulations, Commission Rules, Australian/New Zealand Gaming Machine National Standard and the Tasmanian Appendix to the Australian/New Zealand Gaming Machine National Standard.

4.4.7. An EMS must not enable a gaming machine for play if any of the gaming machine or game parameters do not match the approved configuration in the EMS gaming approvals database.

Enable/Disable Gaming Machine or Venue Based EMS Equipment

4.4.8. An EMS must include functions to enable or disable a gaming machine or any venue-based EMS equipment based on pre-specified events or manual processes.

4.4.9. An EMS must include the capability for an authorised user to initiate manual (ad-hoc) commands to disable any gaming machine or venue-based EMS equipment.

4.4.10. An EMS must include the capability for an authorised user to initiate manual commands to enable any gaming machine or venue-based EMS equipment. Such commands must automatically initiate a software set authentication test of the respective device, and the device may only be enabled if the EMS is satisfied that only approved software sets are operating on that device.

Responding to Gaming Machine Events

4.4.11. An EMS must include a control capability to respond to events from gaming machines, linked jackpot arrangements and venue-based EMS equipment.

4.4.12. An EMS must:

a) Disable a gaming machine after a logic door open is detected;

b) Force gaming machine software set authentication after power up of a gaming machine or venue-based EMS equipment;

c) Force gaming machine software set authentication after a gaming machine logic door is closed (before a gaming machine can be enabled); and

d) Force large jackpot payments to be paid manually (amount to specified by the Commission and configurable within the EMS).

Logic Door Re-seal

4.4.13. An EMS must include a capability for an authorised user to initiate a system command to re-seal a logic door on a gaming machine or linked jackpot equipment.

4.4.14. A system command to re-seal a logic door must only be executed after an EMS has completed authentication of the gaming machine software and game configurations.

4.4.15. Where a gaming machine is participating in a linked jackpot arrangement, an EMS must only allow operation of approved linked jackpot arrangements and parameters.

Licensed Venue Hours of Operation

4.4.16. An EMS must disable all gaming machines and linked jackpot arrangements at each licensed venue outside of the approved gaming operating hours for each venue.

4.4.17. At the start of a licensed venue's operating hours, an EMS must enable gaming machines and linked jackpot arrangements only after the successful validation of software sets and gaming machine/game parameters, as outlined in sections 4.4.3, 4.4.6 and 4.4.7.

Standalone Gaming Machines Not Permitted

4.4.18. Any approved gaming machine must, at all times it is in operational mode, where authorised game play is permitted, maintain on-line communication with the venue EMS host. This requires that:

a) A gaming machine must disable itself when it loses communications with the next point of the EMS for a period longer than 20 seconds;

b) EMS components attached to a gaming machine (such as an interface card or protocol converter) must disable its attached gaming machine, if that component loses communications with the next point of the EMS for a period of longer than 20 seconds;

c) The venue EMS host must disable all gaming machines attached to it, including linked jackpot arrangements operated by it where a venue EMS host loses communications with the central EMS host for a period longer than <down_time_permitted>.

4.4.19. There must be a means to extract meter and event information from each venue EMS host after the down time period to enable further operation of gaming at the venue.

4.5 Monitoring Meters

Gaming Machine Meters

4.5.1. A central EMS host must receive and record the following meter set, as defined in the Australian/New Zealand Gaming Machine National Standard, from every authorised gaming machine in all licensed venues, at least once every day:

a) Master gaming machine meters; and

b) Multi-game meters (for gaming machines operating multi-game software sets).

4.5.2. An EMS must be capable of receiving and storing additional information from gaming machines relative to ante-bet usage, access to gaming machine-based consumer protection measures (such as accessing player information displays) and other harm minimisation measures, where available, through gaming machine communication protocols.

4.5.3. A venue EMS host must receive gaming machine meters as quickly and frequently as supported by the gaming machine communication protocol operating in each gaming machine.

4.5.4. A venue EMS host must create and store a "snapshot" of all gaming machine meters for each gaming machine, and linked jackpot arrangement pool values, in that licensed venue, at least every 15 minutes.

4.5.5. A venue EMS host must receive and store meter sets from its connected gaming machines at least every 20 minutes.

4.5.6. Meter values, including "snapshot" recordings, stored in a venue EMS host must be stored in non-volatile memory that can maintain its memory contents for at least 90 days, in the event of loss of mains power.

4.5.7. All financial meter values from gaming machines must be recorded in cents value. Rounding, or truncation of financial meter values, is not permitted.

4.5.8. All non-financial meters must be recorded in the same base unit value as reported by the respective gaming machine or device (e.g. numeric count of games played, or coins inserted).

4.5.9. A venue EMS host must timestamp each recorded meter set, together with the respective gaming machine floor location and EMS gaming machine identifier (refer to section 4.2).

4.5.10. All gaming machine meter values reported by a venue EMS host to the central EMS host must be gross meter values (as reported by connected gaming machines) and not as incremental values.

Linked Jackpot Arrangement Meters

4.5.11. A central EMS host must record each progressive meter set, defined in the Australian/New Zealand Gaming Machine National Standard, for every linked jackpot arrangement level managed by a venue EMS host in all licensed venues in Tasmania, at least once every day.

4.5.12. A venue EMS host must store meter sets for all linked progressive jackpot arrangements at least every minute and retain the meter information for at least 24 hours, on a rolling basis.

4.5.13. All financial meter values from linked jackpot arrangements must be recorded in cents value. Rounding, or truncation of financial meter values, is not permitted.

4.5.14. All non-financial meters must be recorded in the same base unit value as reported by the respective linked jackpot arrangement (e.g. number of hits of a particular jackpot level).

4.5.15. All progressive meter values reported by a venue EMS host to the central EMS host must be gross meter values and not as incremental values.

Handling of Non-Conforming Meter Values

4.5.16. An approved gaming machine communication protocol supported by an EMS must report gaming machine meters in strict compliance with the definitions of the Australian/New Zealand Gaming Machine National Standard, unless meter values are able to be derived from other meters recorded by a gaming machine and the integrity of information is maintained.

4.5.17. An application must be made to the Commission to consider any meter derivation processes and must be accompanied by an ATF report certifying the suitability of the process.

Time/Date Stamping of Meter Recordings

4.5.18. All transactions from any component of an EMS where meter values are recorded, must be time-stamped with the date and time the meter value was recorded.

4.6 Monitoring Events

Gaming Machine Generated Events

4.6.1. A venue EMS host must receive and record all gaming machine events reported by the gaming machine communication protocol operating in each gaming machine in that licensed venue.

4.6.2. A venue EMS host must record and forward to the central EMS host all logic door re seal commands executed on a gaming machine.

4.6.3. A venue EMS host must retain all gaming machine events for at least 14 days.

4.6.4. Gaming machine events stored in a venue EMS host must be accessible via authorised user functions to provide assistance in audits, investigations and customer disputes.

Linked Jackpot Prize Award Events

4.6.5. A venue EMS host must record complete details for each jackpot prize awarded for any level of a linked jackpot arrangement, including date/time, jackpot identifier, jackpot level, prize value, and the gaming machine which awarded the prize.

4.6.6. A venue EMS host must retain all linked jackpot prize award events for at least 14 days.

4.6.7. Linked jackpot prize award events stored in a venue EMS host must be accessible via authorised user functions to provide assistance in audits, investigations and customer disputes.

Central EMS Host Event Reporting and Recording

4.6.8. The following events must be recorded by a central EMS host and reported to the monitor:

a) Logic area accessed;

b) Software set authentication failure;

c) Gaming machine off-line during approved licensed venue operator hours;

d) Unapproved gaming machine serial number in a licensed venue;

e) Venue EMS host failure;

f) Progressive prize award and prize value, including standalone progressive jackpot prizes;

g) Linked jackpot arrangement parameter changes (such as increment rate, start-out value, current pool amount), including pre and post change values;

h) Linked jackpot arrangement configuration changes (such as adding/deleting gaming machines or commissioning/retiring a linked jackpot arrangement), including pre and post change values;

i) The failure to receive meter values from a gaming machine or linked jackpot arrangement;

j) Linked jackpot prize pool reset; and

k) Gaming machine excessive turnover meter increment.

4.6.9. Events detected in a specific licensed venue must be stored by a venue EMS host for a period of at least six months.

4.6.10. All events, from all licensed venues, must be recorded by a central EMS host and stored for a period of no less than 13 months.

4.6.11. All events must be timestamped with sufficient information to identify the event, and include licensed venue identifier, gaming machine identifier, and linked jackpot arrangement identifier.

Time/Date Stamping of Events

4.6.12. All events recorded and stored by any component of an EMS must be time-stamped with the date and time the event was detected.

4.7 Accounting

Daily Gaming Machine and Progressive Meter Records

4.7.1. An EMS must calculate and store daily meter increments for all meters from all gaming machines reported by venue EMS hosts.

4.7.2. An EMS must calculate and store daily meter increments for all progressive meters from linked jackpot arrangements reported by venue EMS hosts.

4.7.3. An EMS must include processes to automatically "roll-over" any meter.

4.7.4. An EMS must store daily meters in a format that retains gaming machine and linked jackpot arrangement identities for each licensed venue.

4.7.5. An EMS must enable access to, or retrieval of, daily meters for a period of at least three years.

Daily Gaming Machine Gross Profit

4.7.6. An EMS must calculate and store the daily gross profit for every gaming machine in each licensed venue in Tasmania (where applicable), which is to be calculated by deducting from the total amount wagered on gaming machines in that period less the sum of all winnings paid.

4.7.7. An EMS must store daily gaming machine gross profit values in a format that retains gaming machine identity for each licensed venue.

4.7.8. An EMS must enable access to, or retrieval of, daily gaming machine gross profit values for a period of at least three years.

Licensed Venue Daily Gaming Machine Gross Profit

4.7.9. An EMS must calculate and store the daily aggregate gaming machine gross profit for each licensed venue in Tasmania (where applicable).

4.7.10. An EMS must store licensed venue daily gaming machine gross profit values in a format that retains gaming machine identity for each licensed venue.

4.7.11. An EMS must enable access to, or retrieval of, licensed venue daily gaming machine gross profit values for a period of at least seven years.

4.8 Reporting

General Reporting Capabilities

4.8.1. An EMS must be able to provide reporting for the following areas:

a) The financial activity and transactions of all gaming in licensed venues;

b) Significant integrity events relative to the operation of gaming in licensed venues;

c) Access to, or usage of, consumer protection features on gaming machines (where gaming machines and/or gaming machine communication protocols supply such data); and

d) Regulatory reports, as required.

Commission Reporting Requirements

4.8.2. An EMS must be capable of producing the following reports for the Commission for each licensed venue connected to the EMS:

a) Daily, weekly, monthly, and yearly based financial summary that totals all cash flow for each gaming machine;

b) Gaming machine gross profit;

c) Significant events for each gaming machine, linked jackpot arrangements and EMS components;

d) Installed gaming machine and gaming configuration;

e) Standalone progressive jackpot activity;

f) Linked jackpot arrangement configuration and activity;

g) Gaming machine return to player, including variance from theoretical return to player values for each gaming machine;

h) Individual game performance for games that are part of an approved multi-game set (including ante-bet / non-ante-bet performance where data is reported to the EMS);

i) Gaming machine operating hours; and

j) Gaming machine reconfiguration (including gaming machine movement).

4.8.3. An EMS must facilitate a range of flexible, user configured options for each report type, such as date ranges, licensed venue (e.g. individual, regional, selected venues, and licensee), and gaming machine(s).

4.8.4. An EMS must allow for flexible reporting modules to support extensible reporting options.

4.8.5. An EMS must provide information in a format as required by the Commissioner of State Revenue. Suitable file formats include:

a) Fixed file;

b) CSV;

c) XML (represented by defined XSD attributes).

The EMS must be able to transfer information by an automated "file push" or "file pull" process.

4.8.6. A monitor must make a written application to the Commission for any alterations or adjustments to reports.

4.8.7. A monitor must implement procedures to verify the integrity of reports so as reports remain certified and approved.

4.8.8. A monitor must offer the Liquor and Gaming Branch online electronic access to EMS reporting modules in a secure manner from a variety of remote (to the EMS) locations.

4.8.9. The Commission must be able to generate reports after the close of trading day from an EMS.

Licensed Venue Operator Reporting Requirements

4.8.10. A central EMS host and venue EMS host must be capable of producing the following reports for a licensed venue operator, and the Commission on request:

a) Gaming machine and game configuration reporting, including floor location number, gaming machine manufacturer, gaming machine type, installed game(s) and operating game parameters;

b) Linked jackpot arrangements and parameter reporting for any linked jackpots operated by the licensed venue operator;

c) Periodic gaming machine meter reports that allow the licensed venue operator to specify date ranges for the reports to provide reporting of stroke, turnover, credits won, cash in, cash out, and cancel credit for each gaming machine, including the gaming machine floor location;

d) Jackpot reconciliation reports detailing the estimated current jackpot pool amount from contributing gaming machine turnover, jackpot prizes paid and jackpot reset amounts;

e) Cash reconciliation reports to assist the licensed venue operator in the management of coin hoppers and estimated coin clearance amounts;

f) Excessive gaming machine meter movement reports;

g) Gaming machine significant event reports that allow the licensed venue operator to specify the significant event reporting period; and

h) Gaming machine gross profit reports that allow a licensed venue operator to specify the reporting period for reporting calculated gross profit for each gaming machine and a venue gross profit total for all gaming machines.

4.9 Terminal Financial Adjustments

4.9.1. A monitor must establish and maintain policies, procedures, and standards for the loss of gaming machine, or linked jackpot arrangement soft meter data, due to malfunctions or maintenance activities.

Master Meter Reset

4.9.2. An EMS must be able to identify and facilitate adjustment to central EMS host records in the event master resets have occurred for gaming machines, linked jackpot arrangement configurations, or venue-based EMS hosts.

4.9.3. To support any adjustment process, an EMS must be able to retrieve the last valid meters stored within the EMS before a master reset occurred.

4.9.4. An EMS must provide a secure method for the entry of manually derived metering information to update and rectify metering errors. The method of manual entry must be subject to strict security controls and the EMS must perform reasonableness checks against the last meter values automatically recorded by the EMS.

Terminal Financial Adjustment Procedures

4.9.5. A monitor must have in place the following policies and procedures for the adjustment to meter values:

a) Adjustments must only be performed by authorised personnel;

b) Access to EMS functions that facilitate terminal financial adjustments are limited to authorised users in accordance with approved EMS monitoring procedures;

c) Control and monitoring of adjustments (such as multi-part password control shared with Liquor and Gaming Branch Inspectors);

d) Manual records of adjustment values must be kept by a monitor; and

e) The EMS must maintain system records of all terminal financial adjustments, and these must be accessible via EMS reports.

4.10 Linked Jackpot Equipment Monitoring

General

4.10.1. The Commission's Linked Jackpot Equipment Technical Standards document set out requirements for linked jackpot equipment connected to gaming machines in Tasmania.

4.10.2. An EMS must monitor all linked jackpot equipment connected to gaming machines in licensed venues that the EMS is responsible for monitoring.

4.10.3. EMS monitoring of linked jackpot equipment must include:

a) Authentication of linked jackpot equipment software;

b) Authentication of linked jackpot arrangement configuration(s);

c) Recording meters from linked jackpot equipment; and

d) Detecting and recording events from linked jackpot equipment.

Authentication

4.10.4. An EMS must authenticate the software set of any linked jackpot equipment operated by, or connected to it, following the requirements set out in section 4.4.2 of these standards, prior to enabling that linked jackpot equipment to operate.

4.10.5. An EMS must verify that any linked jackpot arrangement configuration set up in linked jackpot equipment matches the approved configuration held in the EMS gaming approvals database.

4.10.6. Failure of any linked jackpot equipment authentication steps, including configuration verification, must result in a significant event being recorded by an EMS and that linked jackpot equipment must be disabled from operating any linked jackpot arrangements until successful authentication.

Meters

4.10.7. An EMS must receive and record meters from linked jackpot equipment in accordance with section 4.5 of these standards and the Commission's approved Linked Jackpot Equipment Technical Standard.

Linked Jackpot Equipment Events

4.10.8. An EMS must detect and record events from linked jackpot equipment in accordance with section 4.6.8 of these standards and the Commission's approved Linked Jackpot Equipment Technical Standard.

4.11 Financial Day

4.11.1. An EMS must implement a financial day where all recorded meters, events, and derived data for a 24 hour period, are reportable against that financial day (e.g. a 24 hour period from 6am until 5:59am the following day).

4.11.2. Only one financial day period can operate across all gaming machines, linked jackpot arrangements and licensed venues connected to an EMS operated by a monitor.

4.11.3. A venue EMS host connected to an EMS must implement "end of day" at the same time across all connected licensed venues.

4.11.4. A venue EMS host must include a process to accurately collect all meters and events for gaming machines and linked jackpot arrangements within the appropriate financial day.

4.11.5. A central EMS host must report all instances where it fails to receive end of financial day meters from a venue EMS host for a gaming machine or a linked jackpot arrangement.

4.12 Other Services

4.12.1. An EMS must be able to securely provide the following services or be capable of securely interfacing with external systems to provide the services:

a) Card-based gaming;

b) Player loyalty;

c) Player pre-commitment and consumer protection; and

d) EMS connection with licensed venue operator owned equipment used for in-venue gaming machine reporting or other data reporting.

4.12.2. All gaming equipment and external systems participating in the provision of services outlined in section 4.12.1 must use techniques that enable the authentication of its components and use secure communications.

4.12.3. A monitor or supplier must provide an ATF report to the Commission, certifying the security of communication and authentication techniques used by services outlined in section 4.12.1.

4.12.4. Gaming equipment and external systems that have been approved by the Commission for use in connection with an EMS to provide the services listed in section 4.12.1, must not allow unauthorised access to EMS software or its records.

5. EMS Operations

5.1 EMS Information Security Management System

5.1.1. A monitor must operate and maintain an information security management system that is compliant with the requirements of ISO/IEC 27001:2013 standard, or equivalent.

5.1.2. In its application to the Commission for approval to use an EMS, a monitor must submit detailed policies, procedures and standards that will be adopted and implemented to demonstrate compliance with ISO/IEC 27001:2013 or equivalent.

5.1.3. A monitor must have in place the following key controls for its information security management system:

a) System access (e.g. use of passwords or equivalent, access rules by role);

b) Detection, prevention and correction of security configuration changes or breaches;

c) Security and configuration management of media for the storage of data;

d) Prevent hacking and unauthorised access to the EMS;

e) Timely application of manufacturer recommended operating system, database and security patches;

f) Making reasonable efforts to enable confirmation that operating systems used to provide EMS services are patched and configured in a timely manner to maintain system integrity and protect against unauthorised access;

g) Mechanisms for authorised personnel from an EMS supplier or maintainer to gain access to EMS software, systems, infrastructure, and data;

h) Access restriction to functions that enable system parameter changes, installation of new software versions, and other critical functions as determined by the Commission; and

i) Periodic independent system and network vulnerability testing and penetration testing.

5.2 Systems Audit

5.2.1. A monitor must facilitate regular audits of the EMS by the Commission, including, but not limited to:

a) Logical access security and control such as user access creation, user and access privileges reviews, generic accounts security and controls, remote access control and management;

b) Physical and environment security such as data centre access controls (where used), security, and control;

c) System integrity such as approved components baseline verification for compliance, source code integrity, regular monitoring of critical activities of the system and its components with preventive, detective, and corrective controls in place;

d) Data and information security and integrity such as database security and control, financial data integrity, customer data and information integrity;

e) Maintenance of gaming machine, licensed venue, and linked jackpot arrangement configuration information;

f) Reconciliation of approved game manifests held within the EMS gaming configuration database;

g) Networks and communications security such as regular network control document reviews, prevention, detection, and correction measures for relevant security breaches;

h) Software, hardware and network change management and deployment such as emergency change and configuration management;

i) Problem and incident management including significant events management;

j) System availability such as backup security and controls by regular testing of retrieval and restore from backup devices, storage management records;

k) Business continuity management such as disaster recovery and business continuity planning, testing and documentation;

l) Asset management such inventory management of approved components;

m) System interfaces and peripheral equipment integrity;

n) Accountability maintained by appropriate segregation of duties;

o) Adequate audit trail maintained for accountability, reconstruction, intrusion detection, problem detection;

p) System and audit log monitoring including appropriate procedures for follow-up and corrective action; and

q) Availability of adequate policies, procedures, and standards, which are regularly followed, maintained, and kept up to date.

5.3 Disaster Recovery and Business Continuity

5.3.1. A disaster recovery site must meet the standards required for the primary site, as set out in these standards.

5.3.2. A monitor must have a demonstrated disaster recovery and business continuity ability through adequate backup and recovery mechanisms (including total capacity to cope with peak load, fault tolerance, security, and control).

5.3.3. A monitor must establish and maintain policies, procedures and standards for business continuity and disaster recovery.

5.3.4. A monitor must establish and maintain a business continuity plan, and a disaster recovery plan.

5.3.5. A monitor must establish and maintain a comprehensive disaster recovery test plan, including a schedule for testing, which must be supplied to the Liquor and Gaming Branch upon request, and conduct disaster recovery testing in accordance with the plan.

5.3.6. In the event of a disaster, there must be a method of ensuring that all data and information related to an EMS, transactions and player entitlements (since the last backup and the transaction log) can be rebuilt up to the point of the disaster.

5.3.7. Copies of all daily database backups must be retained at a secure location, other than the primary site, and the secure location must have security policies, procedures and standards equivalent to that required of the primary site.

5.3.8. There must be periodic back-ups (at least daily) of the variable database files on the central components of EMS storage devices.

5.3.9. A monitor must have the location of disaster recovery sites approved by the Commission.

5.4 Transaction Logging

5.4.1. A central EMS host must maintain a log file or database record (recording a date and time stamp) of all significant events received from gaming machines, linked jackpot arrangements and venue EMS hosts.

5.4.2. A complete log of transactions since the last EMS backup must be maintained at a disaster recovery site.

5.4.3. All log files or databases used for transaction logging must be duplicated using a secure storage methodology.

5.4.4. All transactions and events must be written to the log in the order that they occurred.

5.4.5. It must not be possible to add to, amend, "write over" or delete any transaction, record or data contained in the log of existing records.

5.4.6. A monitor must provide the Commission with a certificate from an ATF stating that in its opinion, significant events that are required to be logged and the method of logging will be effective in a disaster recovery situation.

5.5 On-line Accessibility to EMS Data and Reports

5.5.1. An EMS must maintain all records of data (including meter readings, events, accounting information and gaming configuration database) with immediate on-line accessibility, for a period of at least 13 months.

5.6 Long Term Access to EMS Data and Reports

5.6.1. A monitor must maintain accessibility to all EMS records of data (including meter readings, events, accounting information and gaming configuration database) for a period of at least three years (e.g. via an off-line archive capability).

5.6.2. It must be possible to generate reports using historical data for periods up to at least three years (e.g. long term return to player analysis).

5.7 EMS Data Backup

5.7.1. An EMS must incorporate a method to backup all data, records and transaction logs at least once per day to allow recovery in the event of an interruption to, or failure of, the central EMS host.

5.7.2. EMS data backups must be retained by the monitor for a minimum period of seven years.

5.7.3. EMS data backups must be accessible to the monitor and in a usable state to support EMS recovery functions within a two hour time limit.

5.7.4. EMS data backups must be securely stored and only accessible by authorised personnel.

5.8 EMS Recovery

5.8.1. In the event of a failure, all EMS components must be able to recover all critical data and records from the time of the last back-up to the point at which the failure occurred.

5.8.2. An EMS must be able to recover from unexpected restarts of its central computers or any of its components.

5.8.3. EMS data storage must be secure and incorporate fault tolerant, mirrored, storage media.

5.9 Retention of Unclaimed Monies

5.9.1. Retention of unclaimed money by an EMS must be treated in accordance with the Act.

5.9.2. A monitor must maintain a register of unclaimed prize monies.

5.9.3. An EMS must secure information relating to unclaimed monies so that only authorised users are permitted to run reports, or access details such as venue name, date, amount, gaming machine or linked jackpot arrangement identifier.

5.10 Date and Time

5.10.1. A central EMS host must maintain a central clock that reflects the date and time in Tasmania.

5.10.2. An EMS central clock must automatically manage transition between standard time and daylight saving time at the prescribed date(s) and time(s) in Tasmania without compromising the integrity or accuracy of any data collection or reporting.

5.10.3. An EMS central clock must be maintained to an accuracy of one second.

5.10.4. EMS components connected to a central EMS host must maintain a clock that accurately reflects the date and time of the EMS central clock.

5.10.5. Where an EMS component determines that its clock is inaccurate, there must be an automatic method of re-synchronising that clock from the EMS central clock.

5.11 EMS Upgrades

Central EMS Host Software Upgrade

5.11.1. Upgrades to central EMS host software must be undertaken in a manner that reduces impacts on EMS functionality and licensed venues. If impacts are unavoidable, they must be undertaken is in accordance with approved service level agreements.

5.11.2. A monitor must seek approval from the Commission to upgrade central EMS host software.

5.11.3. Any request to implement a central EMS host software upgrade must include details of the upgrade strategy, such as using the EMS test system for process testing, estimated overall time for upgrade and full service restoration, planned time of day for the upgrade (utilising as much time as possible outside of licensed venue trading hours).

5.11.4. Any request for complex or significant central EMS host software upgrades, such as operating system or database changes, or changes that impact EMS records, must include a recommendation from an ATF confirming that the upgrade processes are fulsome and adequate.

Venue Based EMS components

5.11.5. Distribution of software upgrades for venue-based EMS components (such as venue EMS host, gaming machine interface cards, and protocol converters) must be possible via the EMS wide area network.

5.11.6. Distribution of software upgrades for venue-based EMS components must be possible in "background" mode without interrupting monitoring transactions between licensed venues and the central EMS Host.

5.11.7. Initiation of a software upgrade for venue-based EMS components must only be triggered by authorised users on the central EMS host, in accordance with approved procedures.

EMS Emergency Situations

5.11.8. The Act does not permit the installation or operation of EMS software or components that have not received prior approval from the Commission.

5.11.9. Any modification of approved EMS software to resolve catastrophic failure of the EMS must not occur without prior approval from the Commission

5.11.10. In the event of serious or catastrophic failure of the EMS, the monitor must implement disaster recovery processes.

6. Network and Communication Requirements

6.1 General

Communications Protocol

6.1.1. All communication between components of an EMS must be via a protocol-based communications scheme.

6.1.2. All communication protocols must include error control, flow control and link control (for remote connection) capabilities.

6.1.3. All communication protocols must make use of cyclic redundancy checks (CRCs) or the equivalent.

6.1.4. All communication protocols must not solely rely upon parity or simple checksum byte to perform validation of transmitted data.

6.1.5. All communication protocols must be able to withstand varying error rates.

On-line Real Time Communications

6.1.6. Game play on a gaming machine must only occur when the EMS has enabled the gaming machine for play and the venue EMS host is in direct communication with that gaming machine. Acceptable communication failure periods for gaming machines are listed under section 4.4.18 of these standards.

Network Cabling Requirements

6.1.7. The following standards must be met in an EMS network:

a) The Australian Government Information Security Manual;

b) Australian Communication and Media Authority Standard AS S008 – Telecommunications Technical Standard (requirements for customer cabling products); and

c) Australian Communication and Media Authority Standard AS S009 – Installation requirements for customer cabling.

Network Device Security

6.1.8. Access to all network devices used by an EMS must be secured and controlled by the monitor.

6.2 Cryptographic Data Security

Introduction

6.2.1. For the purposes of this section:

a) Cryptographic data security refers to the protection of critical communication data from eavesdropping and/or illicit alteration.

b) Eavesdropping protection is achieved by using a demonstrably secure encryption algorithm.

c) Protection against illicit alteration is achieved by using a demonstrably secure message authentication code algorithm although some encryption algorithms also provide this protection.

Requirement for Cryptographic Data Security

6.2.2. Except as approved by the Commission on a case-by-case basis, the following requirements related to cryptographic data security apply:

a) Other than within an EMS computer room, cryptographic data security must apply to all critical data that traverses data communications lines.

b) Cryptographic data security must apply for all critical data communication transfer between all components of an EMS at a licensed venue, and between a licensed venue and the EMS central site.

c) The following critical data items must be encrypted by a demonstrably secure encryption algorithm:
   i. Encryption keys, where the implementation chosen requires transmission of keys;
   ii. PINs;
   iii. Passwords;
   iv. Commercially confidential information, including but not limited to gaming configuration data, meters, events, and information related to government revenue;
   v. Vital transactions related to the operation of the EMS; and
   vi. Email or equivalent communication methods that contain any of the above data or information.

d) A monitor must provide notification to the Commission of any software or tools that are able to decrypt or reveal critical data.

e) The following critical data items must use a demonstrably secure message authentication algorithm:
   i. Software uploads and downloads of any security related software
   ii. Transfers of money to/from player accounts
   iii. Transfer of money between components of an EMS

f) There must be a password protected and secure function to disable encryption to handle circumstances where difficulty with communications is encountered. The process for password protection must be approved by the Commission and must include mandatory involvement of staff from the Liquor and Gaming Branch completing steps in password entry (or a secure logical equivalent).

g) Disabling of encryption must only occur with the prior approval of the Commission.

Encryption Algorithm

6.2.3. The following encryption characteristics must apply to an EMS:

a) Encryption algorithms must be demonstrably secure against cryptanalytic attacks and must confirm to industry standards;

b) The minimum width (size) for encryption keys must conform to industry standard encryption;

c) There must be a secure method implemented for changing the current encryption key set; and

d) A current key set must not be used to "encrypt" the next key set. An example of an acceptable method of exchanging keys is the use of public key encryption techniques to transfer new key sets.

Message Authentication Algorithm

6.2.4. An EMS must have the following authentication characteristics in place:

a) Message authentication code algorithms are to be demonstrably secure against cryptanalytic attacks;

b) Message authentication code algorithms are to be designed such that it is feasibly impossible to take a hash value and recreate the original message, "impossible" in this context means "cannot be done in any reasonable amount of time"; and

c) Message authentication code algorithms are to be designed such that it is feasibly impossible to find two messages that hash to the same hash value.

Encryption Keys

6.2.5. Key algorithms to be used to provide cryptographic data security must conform to industry standard encryption and authentication structures.

6.3 Wireless Communication

6.3.1. Wireless communication must not be used unless it has been approved by the Commission and meets the standards set out for wireless communication in the Australian Government Information Technology Security Manual (ISM).

6.3.2. A wireless access point must be physically positioned so that it is not easily accessible by unauthorised individuals.

6.3.3. A wireless access point must not be placed directly onto the licensed venue network unless a secure firewall is in place.

6.3.4. Any request for approval of wireless communication, must be accompanied by an ATF certification.

6.3.5. Wireless network traffic must be secured with additional encryption and/or authentication codes and must meet the requirements for cryptographic data security outlined in these standards.

6.3.6. The keys used to encrypt the communication through the wireless network must be stored in a secure location.

7. EMS Control Documentation

7.1 Retention of EMS Documentation

7.1.1. A monitor must maintain and retain all records pertaining to the design, manufacture, and testing of the EMS.

7.1.2. When submitting a change to the EMS, or any EMS component for approval, a monitor must provide sufficient information and documentation to the ATF, or the Liquor and Gaming Branch upon request, to enable determination that the EMS, or EMS components, are compliant with these standards.

7.2 EMS Baseline Document

7.2.1. A monitor must prepare, in a form acceptable to an ATF, a baseline document that describes the software and hardware of the EMS, interfaces, and any other components that are core to the operations of the EMS as outlined in these standards, including but not limited to:

a) Operations and monitoring of gaming machines, and related transactions to and from gaming machines;

b) Functions that are related to the capture, processing, and storage of critical data;

c) Functions required by any regulatory and/or government bodies;

d) Primary source of storing the critical data in relation to EMS activities; and

e) Structured reporting in relation to the ongoing operation of the EMS.

7.2.2. The baseline document must include details and specifications for all EMS components, including:

a) Hardware platforms;

b) Operating systems;

c) Application files, critical macros, and scripts;

d) Interface modules and databases use by EMS applications;

e) Venue EMS host;

f) Gaming machine interface devices (if used by the EMS); and

g) Communications devices that interface with a venue EMS host.

7.2.3. To establish a baseline document, agreement must be reached with the ATF regarding the directories in which application files will be located on the central components of EMS computers. Files that cannot be verified because they change frequently are not required to include functionality that would be in the baseline, nor be stored in system application directories.

7.2.4. The baseline document must include a method to verify the baseline components to confirm that the configuration of the EMS is operating in an approved state. The EMS must be configured so that any baseline components residing on storage devices or in the memory of the EMS, are only executable for the EMS.

7.2.5. A monitor must require the ATF who performed the baseline check to provide a certificate to the Commission stating that the baseline document meets all the requirements of these standards.

7.2.6. After its initial approval, any proposed changes to any baseline component or the baseline document must be certified by an ATF and submitted to the Commission for approval.

7.3 EMS Network Control Document

7.3.1. A monitor must prepare, in a form acceptable to an ATF, a network control document that describes the inbound and outbound firewall rules for data traffic between devices in the EMS baseline (as described in the EMS baseline document), including edge devices.

7.3.2. The network control document must describe the network topology of the EMS detailing the interconnection of components within the network and the types of connection between the components that is permitted.

7.3.3. A monitor must require the ATF who performed the network control check to provide a certificate to the Commission certifying that the network control document meets all the requirements of these standards.

7.3.4. After its initial approval, any proposed changes to any network component or the network control document must be certified by an ATF and submitted to the Commission for approval.

7.4 EMS Master Management Control Document

7.4.1. A monitor must prepare and maintain an EMS master management control document and submit this to the Commission for approval.

7.4.2. An EMS master management control document must include the following:

a) The EMS baseline document;

b) The EMS network control document;

c) The procedure for handling system changes in general;

d) The procedure for handling emergency changes;

e) The procedure for maintaining the EMS master management control document, including any emergency changes;

f) Any other operation or procedure that is relevant to securing control of the EMS;

g) Any changes implemented in the last 12 months, or in comparison to the last EMS master management control document; and

h) The method and mechanisms used to verify that the EMS is operating in an approved state.

7.4.3. A monitor must require the ATF who reviews the EMS master management control document to provide a certificate to the Commission in support of the application for approval.

7.5 EMS Operational Documentation

7.5.1. A monitor must establish and maintain policies, procedures and standards in accordance with the requirements of section 2.1.2 of these standards.

7.5.2. A monitor must establish and maintain internal control policies, procedures, and standards for the operation of the EMS, which must be approved by the Commission.

8. EMS Software Management

8.1 EMS Source Code

8.1.1. A monitor must provide source code for all software and firmware components of an EMS to the representing ATF, or the Commission on request, in an approved machine readable form.

8.1.2. A monitor must clearly identify to the representing ATF, or the Commission on request, any source code that is deemed to be closed source software.

8.1.3. Closed source software must not be used in functions that are central to the operation of an EMS, which include:

a) Installation and configuration of gaming machines;

b) Monitoring and recording of gaming machine meters, transactions and significant events;

c) Protection of non-volatile memory;

d) Jackpot control and monitoring functions;

e) Security monitoring; and

f) Gaming machine and EMS, including venue EMS software verifications.

8.1.4. A monitor must have provisions in place to allow appropriate access to the closed source code to the representing ATF, or the Commission on request, for the purpose of investigating software faults.

8.1.5. All arrangements with closed source software vendors must be provided to the Commission, or the representing ATF on request.

8.1.6. All source code submissions must identify each module, revision number, brief description of functions performance and update history.

8.1.7. Source code must contain adequate comments to understand the functions and processes of the source code.

8.2 Compilation of EMS Source Code

8.2.1. Source code submissions must include all necessary hardware and/or software tools and instructions to enable an ATF to perform verification of source code with object code.

8.2.2. Source code submissions must also comply with the compilation requirements of the Australian/New Zealand Gaming Machine National Standard.

8.2.3. Software to be formally released to the live EMS environment must have been generated (compiled) using the same process as for testing.

8.3 EMS Source Code Control and Upgrade

8.3.1. Separate approval must be obtained from the Commission for each software version.

8.3.2. A monitor must use software version management tools to assign traceable version numbers to all EMS software components.

8.3.3. Any submission for EMS software approval to the Commission must include version numbers (e.g. 1.1.1) for each software component.

8.4 EMS Software Verification

8.4.1. A monitor must provide a method to the Commission to verify that EMS executable software that has been used during an approval testing process is identical to that which is operating in the live environment.

8.4.2. This verification process must occur:

a) When upgraded software is installed;

b) At the start of each financial day; and

c) When requested by the Liquor and Gaming Branch.

8.4.3. There must be a Commission approved method to determine if unapproved programs, command files, fixed data files, reside on any component of the EMS.

9. Approval Submission Requirements

9.1 General

9.1.1. Any submission to the Commission for approval of an EMS, must include the following:

a) General description of the EMS;

b) Purpose of the submission;

c) Description of the scope of system and operational changes;

d) ATF recommendation of the EMS in accordance with above requirements;

e) The monitors' comments on any conditions included in the ATF recommendation;

f) List of all software versions and associated hash values;

g) List of all relevant hardware and operating systems, including product names, models, and versions;

h) Associated systems that are connected to the EMS;

i) The ATF certified EMS baseline document; and

j) The ATF certified network control document.

9.2 Communication Requirements

Line Isolation and EMI/ESD Immunity

9.2.1. A monitor must supply the following information for each communications interface:

a) Technical means by which line isolation is achieved;

b) Line isolation voltage achieved; and

c) Data communications.

Simulation Software

9.2.2. A monitor must make available to the representing ATF, or the Liquor and Gaming Branch on request, simulation software to enable simulation of all commands and manipulation of all message types between gaming machine games, gaming machine equipment and all EMS components. This requirement applies to all communications between the following physically distinct devices:

a) Gaming machine to venue EMS host;

b) Gaming machine to linked jackpot equipment;

c) Linked jackpot equipment to venue EMS host; and

d) Venue EMS host to Central EMS host.

Protocol Specification and Message Formats

9.2.3. Descriptions and specification documents of all protocols and message formats used or supported by the EMS must be supplied the representing ATF, or the Liquor and Gaming Branch on request, for the following:

a) Gaming machine to venue EMS host;

b) Gaming machine to linked jackpot equipment;

c) Linked jackpot equipment to venue EMS host;

d) Venue EMS host to Central EMS host; and

e) Central EMS host to the Liquor and Gaming Branch's computer systems.

9.2.4. Descriptions of the physical interfaces of these various data communication links must be provided to the representing ATF, or the Liquor and Gaming Branch on request.

9.2.5. Where available, a monitor must provide details of testing tools or devices capable of data communication error generation, protocol emulation, protocol testing and protocol monitoring devices.

9.3 Cryptographic Data Security

9.3.1. The following information must be provided relative to cryptographic data security algorithm(s):

a) Description of the algorithm(s);

b) Theoretical basis of the algorithm(s);

c) Results of any analyses or tests to demonstrate that the algorithm(s) is suitable for the intended application;

d) Rules for selection of keys, if appropriate; and

e) Means of setting and protecting keys, if appropriate.

9.3.2. Information must be supplied to explain the situations during which data encryption and message authentication will be employed.

Communications Transmission Medium and Method of Device Connection

9.3.3. A monitor must provide details of communication transmission medium and device connection to the representing ATF, or Liquor and Gaming Branch on request.

9.4 Local Area Network Access Security

9.4.1. A monitor must provide details to the representing ATF, or the Liquor and Gaming Branch on request, the means of security to prevent illegal access to the in-venue local area network (LAN) in the following events:

a) PC or other device inserted on a LAN; and

b) PC or other device inserted on an unused LAN port of a local or linked jackpot equipment.

9.5 Electronic Monitoring System

EMS Architecture

9.5.1. A monitor must provide an overview of the system design to the representing ATF, or Liquor or the Gaming Branch on request.

9.5.2. A monitor must provide a functional specification of the system to the representing ATF, or the Liquor and Gaming Branch on request.

9.5.3. A monitor must provide detailed design documents (including but not limited to schematics, data flow diagrams, algorithms, data dictionaries, etc.) to the representing ATF, or the Liquor and Gaming Branch on request.

9.5.4. A monitor must provide details to the representing ATF, or the Liquor and Gaming Branch on request, the EMS infrastructure (including hosts, front processors, transactions servers, and network management devices) covering areas such as:

a) Role of the component;

b) Operating system;

c) Specifications (such as CPUs, memory, and disc capacity); and

d) Database technologies.

9.5.5. A monitor must provide details to the representing ATF, or the Liquor and Gaming Branch on request, of the EMS central site and central EMS host location.

9.5.6. A monitor must provide details to the representing ATF, or the Liquor and Gaming Branch on request, of any cloud computing environment intended for the operation of any component of the EMS.

Central Logging

9.5.7. A monitor must provide details of where and how information is stored throughout the system to the representing ATF, or the Liquor and Gaming Branch on request.

9.5.8. A monitor must be able to identify and report what information is stored by the system for each separate gaming equipment type.

Password Protection

9.5.9. A monitor must provide details of password protection systems and associated algorithms utilised by the EMS to the representing ATF, or the Liquor and Gaming Branch on request.

Transaction Logging

9.5.10. A monitor must provide details describing the method of transaction logging used to the representing ATF, or the Liquor and Gaming Branch on request.

Encryption of Stored Data

9.5.11. A monitor must provide the following information to the representing ATF, or the Liquor and Gaming Branch on request:

a) Description of the algorithm;

b) Theoretical basis of the algorithm;

c) Results of any analyses or tests to demonstrate that the algorithm is suitable for the intended application;

d) Rules for selection of keys; and

e) Means of setting and protecting keys.

9.5.12. A monitor must supply information to explain the situations during which encryption of data files will be employed to the representing ATF, or the Liquor and Gaming Branch on request.

PIN Management

9.5.13. A monitor must provide the following information to the representing ATF, or the Liquor and Gaming Branch on request:

a) Description of the PIN creation algorithm;

b) Theoretical basis of the algorithm; and

c) Results of any analyses or tests to demonstrate that the algorithm is suitable for the intended application.

9.5.14. A monitor must provide information to explain the implementation of PIN creation.

User Interface, Documentation and Reporting

9.5.15. A monitor must provide operator's manuals to the representing ATF, or the Liquor and Gaming Branch on request.

9.5.16. A monitor must provide copies to the representing ATF, or the Liquor and Gaming Branch on request, of all standard reports produced by the system and describe how these are generated.

9.5.17. A monitor must provide system administrator manuals to the representing ATF, or the Liquor and Gaming Branch on request.

9.5.18. A monitor must provide operator's procedures manuals to the representing ATF, or the Liquor and Gaming Branch on request.

Link to Liquor and Gaming Branch Computing Facilities

9.5.19. A monitor must provide details to the Liquor and Gaming Branch on the manner in which it is proposed this facility is provided.

9.5.20. A monitor must provide to the Liquor and Gaming Branch any special procedures to be followed when using the facility.

9.5.21. A monitor must provide details of the hardware, software and data communications facilities that will be made available to support this link.

9.5.22. A monitor must provide details of the online access for the Liquor and Gaming Branch to the EMS.

Test System

9.5.23. A monitor must provide access to any integration test ("dummy live") environment.

9.5.24. This must include load simulators together with quantities (sufficient for load testing) of all varieties of gaming equipment and monitoring equipment, all configured and functioning in a full live and operational manner.

9.5.25. EMS test system equipment must be configured by the monitor to operate in a manner that reflects the production EMS environment.

9.5.26. A monitor must operate an EMS test system that uses the same EMS software versions approved and operating in the production EMS environment, to enable ATF testing and Commission approval.

9.5.27. A monitor must provide gaming machine protocol simulators to the representing ATF, or the Liquor and Gaming Branch on request, to enable the observation of gaming machines and the EMS in different operational scenarios.

Submitted Equipment

9.5.28. Any equipment under test must have operating software during the tests and the effects, if any, on the correct functioning of the software must be assessed as part of the tests.

9.5.29. Any equipment that is submitted for testing must be a production standard model and must be in "normal operation" during the test, including communication with an EMS or approved simulator (where the equipment employs some form of data communications).

10. Glossary

Term or Abbreviation	Description
Act	*Gaming Control Act 1993.*
ATF	Accredited Testing Facility approved by the Tasmanian Liquor and Gaming Commission and listed on the Roll of Recognised Manufacturers, Suppliers and Testers of gaming equipment under section 71 of the *Gaming Control Act 1993.*
Baseline Document	An approved document that describes the software and hardware of the EMS, interfaces, and any other components that are core to the operations of the EMS.
Central EMS Host	Computer equipment where software and databases perform overall control and management of functions of the EMS.
Central Site	The physical location(s) of the Central EMS Host.
Cloud Computing	A service that uses an internet based computing model in which data and/or applications are stored on third party server locations accessed from the internet, or as otherwise referred to as "the cloud".
Commission	The Tasmanian Liquor and Gaming Commission.
Communication Protocol	A communication specification that defines requirements for data interchange between devices, such as electronic gaming machines and monitoring systems.
<down_time_permitted>	A system parameter that can be extended or shortened but only after approval has been granted by the Commission. The approved default value of <down_time_permitted> is 48 hours.
EGM	Electronic gaming machine.
EMC	Electromagnetic compatibility.
EMI	Electromagnetic interference.
EMS	Electronic monitoring system.
ESD	Electrostatic discharge.
Hash value	A hash value is a numeric or alpha numeric value of a fixed length that uniquely identifies data.
ICT	Information and communication technology.
ISMS	Information security management system.
ISM	Australian Government Information Technology Security Manual.
Licensed Monitoring Operator	A monitoring operator approved under section 48O of the Act.
Licensed Venue	Casino, hotel or licensed club.
Linked Jackpot Arrangement	An arrangement whereby two or more gaming machines or gaming devices are linked to a device that receives data from each linked machine and records any jackpot payable.
Linked Jackpot Equipment	A jackpot meter, payout display, linking equipment, computer equipment, programming, or other device (other than a gaming machine) forming, or capable of forming, part of a linked jackpot arrangement.
Liquor and Gaming Branch Inspector	Means a person appointed to be an inspector in accordance with section 128 of the *Gaming Control Act 1993* and section 209 of the *Liquor Licensing Act 1990.*

Term or Abbreviation	Description
Logic Area	A locked cabinet area (with its own locked door) that houses electronic components that have the potential to significantly influence the operation of the gaming machine or linked jackpot equipment.
Monitor	A licensed monitoring operator or a casino operator.
Network Control Document	A document that describes the inbound and outbound firewall rules for data traffic between devices in the EMS baseline (as described in the EMS baseline document), including edge devices.
Help Desk	A Help Desk facility accessible by hotel and licensed club operators seeking advice or support in relation to the operation of the EMS at their venue.
Pre-commitment	A consumer protection measure whereby pre-set limits on time, frequency, or money spent gambling are registered by players prior to the start of play. • Mandatory pre-commitment requires player registration of pre-set limits before permitting participation on gaming machines to prevent players spending more money than they have pre-committed for a period. • Voluntary pre-commitment does not require mandatory participation, however, allows players to optionally register time, or money spent limits to track and inform them of their expenditure on gaming machines.
Software Set	The combination of software components required for a device's operation (for example, a software set may consist of firmware, shell and game software components).
Source Code	The set of instructions and statements written by a programmer using a computer programming language. This code is later translated into machine language by a compiler. • Open source code refers to software for which source code is available. • Closed source code refers to software provided by a third party, and where source code is not accessible under the terms of the software licence.
Standalone Progressive Jackpot	A jackpot where operation participation, maintenance and control of the jackpot, including selection of the jackpot win criteria, is performed by a single gaming machine.
Venue EMS Host	The primary EMS computer located in a licensed venue (sometimes called a site controller).
WAN	Wide area network.

GPO Box 147, HOBART TAS 7001
Phone: (03) 6166 4040
Email: gaming@treasury.tas.gov.au Visit: www.treasury.tas.gov.au