Table Gaming Management System Technical Standards

Ver 1 4 December 2017

Tasmanian Liquor and Gaming Commission

Tasmania

Table of Contents

1 Introduction

1.1 Objective

1.1.1 The objective of this standard is to ensure that Table Gaming Management Systems (TGMS) and related equipment, operated in Tasmania, are designed to:

- ensure the integrity and fairness of the system;
- ensure the security and auditability of the system and associated equipment;
- be auditable; and
- minimise the potential for harm from gambling.

1.1.2 To ensure, to the greatest extent reasonably possible, the integrity of gaming, a TGMS used in Tasmania should only be operated in casinos by the Casino Operator. This does not prevent Casino Operators from obtaining a system from an external supplier.

1.1.3 The offering of a TGMS requires the approval of the hardware and software, within the supplier's control, that deliver the system and the approval of Internal Controls - the Casino Operator's documented system of procedures for operating the system and ensuring security of the system. This document does not cover internal controls but in describing TGMS requirements assumes that effective Internal Controls are in place.

1.2 Scope and Purpose

1.2.1 The scope and purpose of this document is to describe guidelines for the functionality of a TGMS that may be approved from the Commission's viewpoint, bearing in mind the overarching object in the relevant gaming legislation and other adopted standards.

1.2.2 The process for the approval of the proposed product will be determined by the Commission, in consultation with the supplier. It is expected that Accredited Testing Facilities (ATF) will play an integral part in the testing of the TGMS.

1.2.3 It should also be noted that compliance with this document does not exempt the supplier and Casino Operator from compliance with other laws (e.g. laws relating to privacy, consumer protection, prohibited content, copyright and electronic cash transactions).

1.3 Associated Documentation

1.3.1 Potential Suppliers, third party suppliers and system developers should also familiarise themselves with the following to ensure the TGMS suitability:

- Gaming Control Act 1993
- Tasmanian Liquor and Gaming Commission Mandatory Code of Practice
- Tasmanian Liquor and Gaming Commission Casino Licence Rules
- Tasmanian Liquor and Gaming Commission Premium Player Program Rules
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006
- Privacy Act 1988

- ISO/IEC 27002:2013 Information Technology – Security Techniques - Code of practice for information security controls

1.4 Copyright

2 General

2.1 Configuration and Security

2.1.1 The TGMS must be configured in a manner approved by the Commission. The system must be able to interface (either directly or using an application program interface (API) to export/import information) with all casino table games and tables, automated table games and jackpot systems operating in conjunction with table games.

2.1.2 The functions of cashier, dealer, inspector and gaming supervisor must be isolated with separate security levels.

2.1.3 An approved change control system and/or joint password controls must be in place.

2.2 Access

2.2.1 The system must have swipe card (or similar) facilities to identify all users.

2.2.2 The system must include contemporary devices (e.g. touch screen monitors/tablets) to enable entry of data at the gaming tables.

2.3 Table drop

2.3.1 The system must record the table drop electronically and electronically lock assigned drop boxes to tables.

2.4 Chip control

2.4.1 The system must control the total stock of cashable chips including those assigned to the table floats. All chip movement to and from the cage, floats and tables will be monitored through the TGMS.

2.5 Registered play

2.5.1 The system must have the capability of supporting registered play and recording player gaming activity, both manually and electronically via registered cards where required by the Commission.

3 Hardware/Software

3.1 Approval

3.1.1 All hardware and software must meet minimum requirements (as verified by an ATF) and the approval of the Commission.

3.2 Requirement for Encryption

3.2.1 Where sensitive data is being passed over communication lines (physical or wireless), such data must be encrypted. Examples of sensitive data that require encryption are PINs, passwords, and encryption keys, including any information that if made public could compromise the security of the TGMS.

3.2.2 Sensitive data must be encrypted on an end-to-end basis (i.e. the data must never appear on a LAN or WAN in an un-encrypted form). This includes sensitive data transmitted between computer systems within a Casino Operator's premises.

3.2.3 Sensitive data transmitted between systems within a single secure data centre need not be encrypted.

3.2.4 Sensitive data transmitted between systems that are located within separate secure data centres need not be encrypted if the communications path is physically secure and cannot be accessed by unauthorised people.

3.2.5 Encryption systems are to be demonstrably secure. Only published, public, encryption algorithms and protocols may be used and must have a demonstrated track record against attacks and history of reliable performance.

4 Central Site Requirements

This section describes requirements for the central site (host), including reporting, data recovery and software version controls.

4.1 System Documentation

4.1.1 The Casino Operator must have a security policy covered in its internal control and accounting procedures.

4.1.2 A system baseline network policy document defining the system network topology and defining the communications which take place between devices in the system, must be maintained.

4.1.3 The TGMS supplier must provide adequate documentation to the Casino Operator to configure, maintain and troubleshoot the TGMS without needing the system supplier's guidance.

4.2 TGMS Reporting Capabilities

4.2.1 The system must have the ability to generate regulatory reports as requested by the Commission.

4.2.2 Any alterations or adjustments to reports must be approved by the Commission and the Casino Operator must provide a written explanation for these changes.

4.2.3 There must be the ability to lock and verify reports for the Liquor and Gaming Branch (LAGB) and the Commission's purposes and an ability to be able to verify the system and associated reports remain as certified and approved.

4.2.4 The system must have the capacity to provide the Commission with efficient and seamless "read" access in a sufficient and secure manner in required locations. This "read" access includes access to web based reporting systems that are able to facilitate the generation of reports for periods up to the close of the last trading day.

4.2.5 The Commission must be able to verify the financial activity of all gaming recorded on the TGMS.

4.3 System Backup

4.3.1 There must be a method to backup all data with sufficient frequency to allow recovery in the event of an interruption and data must be backed up for a minimum period of seven years.

4.3.2 If there is sensitive information in the backup data then this must be protected from unauthorised access.

4.4 Data Recovery

4.4.1 The system must retain all data for a minimum of thirteen months.

4.4.2 In the event of a failure, the TGMS must be able to recover all critical information from the time of the last backup to the point in time at which the system failure occurred (no time limit is specified).

4.4.3 The system must be able to recover from unexpected restarts of its central computers or any of its other components.

4.4.4 The operator must have disaster recovery capability sufficient to ensure player entitlements and auditability up to the point of the disaster are protected.

4.4.5 All data must be stored via secure, fault tolerant storage media and must have mirrored storage as a minimum.

4.5 Software Verification

4.5.1 The TGMS supplier and/or its suppliers must provide a method to the nominated ATF to enable verification of the software.

4.6 Source Code

4.6.1 All source code is to be properly commented and contain a change/revision history. If applicable, module descriptions or similar should also be supplied.

4.6.2 All source code central to the operation of the TGMS must be supplied to the Commission or representing ATF where the supplier has the capability, right, and access to provide source code.

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

4.6.4 The Commission may also require that the TGMS suppliers have arrangements with closed source software vendors in place to allow appropriate access to source code by the Commission or representing ATF for purpose of investigating software faults.

4.7 Accounting of Master Resets

4.7.1 The TGMS must be able to identify and properly handle the situation when failures or resets have occurred on other computer systems that affect game outcome, win amount or metering.

4.7.2 The TGMS must be able to retrieve the last valid value of all important parameters stored within the system before the failure or reset occurred.

4.7.3 Adjustments to accounting on the TGMS are subject to strict security control and audit trail.

4.8 Recordable Events

4.8.1 The TGMS must be able to provide a means to view significant events including the ability to search and report on particular event types. This includes system indicator events and trigger events where approved by the Commission.

4.8.2 The TGMS must be able to notify events to the casino operator.

4.9 Audit Trail

4.9.1 The TGMS must have the ability to record and produce a running audit trail showing all transactions in real-time.

4.9.2 Events in the audit trail must be kept on the system for a minimum of thirteen months and backed up for a period of seven years.

4.9.3 The audit trail must be accessible only by authorised personnel.

5 Glossary

Term or Abbreviation	Description
ATF	Accredited Testing Facility accredited by the Tasmanian Liquor and Gaming Commission
Casino	Refers to a premises issued with a Casino Licence under the *Gaming Control Act 1993*
Casino Operator	Refers to a holder of a casino licence granted and in force under section 13 or 28 of the *Gaming Control Act 1993*
Commission	Refers to the Tasmanian Liquor and Gaming Commission (TLGC)
Registered card	One of two player card types available for use with a Card Based Gaming System (the other being unregistered cards)
Supplier	Refers to the supplier of the Table Gaming Management System
TGMS	Table Gaming Management System