Office of Liquor and Gaming Regulation

Identification Scanning System Minimum Technical Requirements

Version 1.5

Queensland Government

For further information, please contact the Office of Liquor and Gaming Regulation on 13 QGOV (13 74 68) or visit https://www.business.qld.gov.au/industry/liquor-gaming

1 Contents

2 Introduction

2.1 Policy

The Queensland Government's Safe Night Out Strategy is a comprehensive plan to deal with alcohol and drug-related violence. The Strategy aims to change the current culture, restore responsibility and respect, and make it clear that bad behaviour will not be tolerated in and around Queensland nightspots. Networked ID scanners have been identified as a necessary tool in the ability of police and licensees to enforce banning notices/orders and also assist police in apprehending offenders.

The Safe Night Out Legislation Amendment Bill 2014 prescribes that venues located in a Safe Night Precinct, authorised to trade after midnight, must scan the ID of persons entering the premises after a designated time. This requires the acquisition of, and participation in, a linked ID scanning system.

2.2 Purpose

The purpose of this document is to provide licensees and manufacturers of identification scanning and storage equipment guidance on OLGR's expected technical capabilities of an ISS.

Compliance with the technical requirements specified in this document does not guarantee compliance to APP11 (security of personal information). Manufacturers and suppliers still need to ensure they meet their obligations under APP11.

2.3 Scope

These requirements are applicable to:

- the hardware and software performing the scanning of identification documentation
- the hardware and software used to identify the patron
- the hardware and software used to operate, maintain or administer the system
- any form of networking capabilities of the system
- storage of information captured by the system (locally and remotely)
- access to information captured by the system (locally and remotely)

2.4 Further Reading

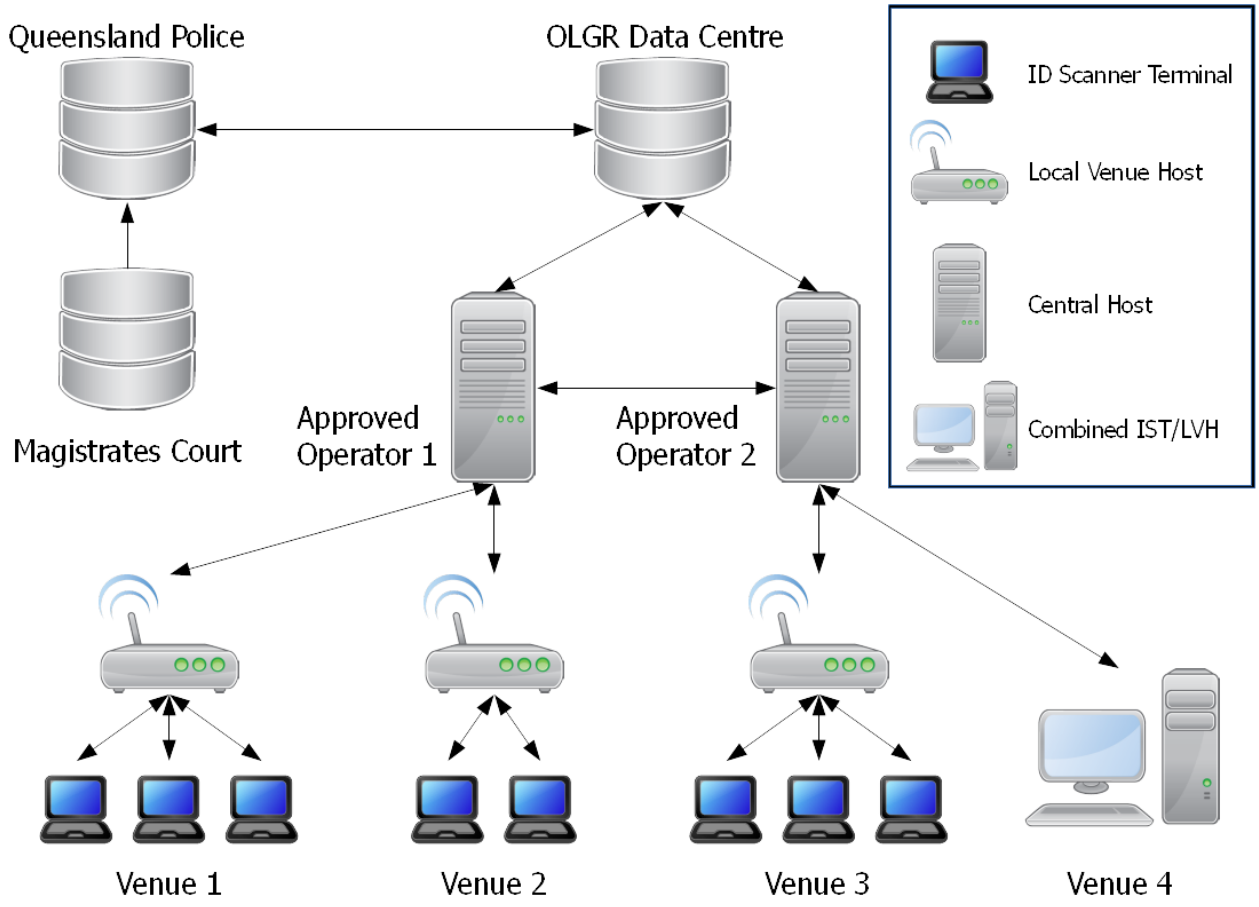
- *Liquor Act 1992* and Liquor Regulation 2002
- *Information Privacy Act 2009*
- Commonwealth *Privacy Act 1988*
- OLGR Approved Seals
- OAIC's Australian Privacy Principles guidelines
- OAIC's Guide to Information Security
- OAIC's Data Breach Notification guide
- OAIC's De-identification of data and information resource

2.5 Abbreviations & Glossary

Identification Scanning System (**ISS**)	An ISS is composed of ISTs, LVHs and CHs. Requirements that are applied to an ISS mean they apply to ISTs, LVHs and CHs.
Identification Scanning Terminal (**IST**)	A device that is capable of scanning a person's identification and provides user functionality.
Local Venue Host (**LVH**)	A device that serves as the central point of communication for ISTs in a venue.
Central Host (**CH**)	A device/server that communicates with venue LVHs and the Queensland Government Data Centre. A CH can only be operated by an Approved Operator.
(**SHA-256)**	A cryptographically secure hash function. Used for software verification.
Official Ban	A Police ban or Court order ban. Refer to banning order, s 173EE *Liquor Act 1992*.
Terminal Operator	A person trained in operating an IST
Queensland Police Service (**QPS**)	
Office of the Australian Information Commissioner (**OAIC**)	
Australian Privacy Principles (**APP**)	
Licensee Ban	A decision of a licensee to ban a particular person from entering the licensee's licensed premises.
Precinct	Refers to a defined Safe Night Out Precinct
Location	Refers to a licensed venue or precinct
eXtensible Markup Language (**XML**)	
SSH File Transfer Protocol (**SFTP**)	
Safe Night Out Precinct (**SNOP**)	
Comma Separated Value (**CSV**)	

2.6 Network Topology

This diagram represents the architectural setup and communication of data across the entire networked arrangement.



3 Technical Requirements

3.1 General

1. Value added services provided by the ISS will not be considered by the Commissioner or captured in the scope of any ISS approval and it is at the ISS provider's discretion to include them. However, all value added services provided by the ISS must not degrade or interfere with core identification and Ban Check functions under any circumstances. Caution must be taken by approved operators and licensee's that any value added services introduced do not breach the *Liquor Act 1992*, Liquor Regulation 2002, *Safe Night Out Legislation Amendment Act 2014*, the *Information Privacy Act 2009 and Privacy Act 1988 (Cth)*.
2. All ISS equipment must be prominently identified with the following information:
   - A manufacturer assigned serial number.
   - Model Number.
   - Device Type (e.g. "Local Venue Host"). This is to prevent confusion when its physical appearance resembles a PC.
   - Sealing point/s (e.g. an arrow with "SEAL" label) and required seal type (if applicable).
3. ISS equipment must be capable of handling extreme environment conditions with an operating temperature range of 5-50 degrees Celsius.
4. Software operating on all ISS devices must be secure.
5. Personal information must be stored in a form that protects it from unauthorised access, modification or disclosure.

3.2 Manuals

1. ISS operating manuals must be supplied to OLGR and the venue.
2. Operating manuals must clearly describe all operations and procedures relating to the ISS.
3. ISS service/maintenance manuals must be supplied to OLGR.
4. Service manuals must contain all technical information, on/off site service/installation procedures and information up to the point of return to manufacturer.
5. The operating and service/maintenance manuals must be approved by OLGR. ISSs will not be approved unless all ISS manuals are considered acceptable by OLGR.
6. The operating and service/maintenance manuals must be version and date controlled.
7. Current manuals must be lodged with OLGR at all times. Manuals must be thorough and easily interpreted.

3.3 Communications

1. All communications must be encrypted with an industry recognised secure encryption standard. This should be the latest version of the standard used unless evidence can be provided why an older version is suitable.
2. Additional security measures may be required based on risk, depending on the type of networking technology implemented.
3. All ISS devices must incorporate and use a firewall. The firewall must be configured to use a whitelist for both inbound and outbound traffic.

4. All ISS devices must have Intrusion Detection software installed and configured to detect, block and log excessive failed logon attempts and/or any other potentially malicious activities.

3.4 Ban Check

3.4.1 General

1. A Ban Check must be performed using:
    a. Surname
    b. Given names
    c. Date of Birth
    d. Photo
2. The ban list will be propagated to LVHs from an Approved Operator's CH (Refer 3.8 Central Host).
3. All ISS devices must be capable of processing Official Bans where a photo has not been provided with the ban list.
4. The IST must be capable of handling multiple bans when a potential match has been raised.
5. The IST must be capable of partial matching of name and date of birth. This is to cater for optical character recognition errors or where a name may slightly differ from the ban details.

3.4.2 Ban Check Process

The IST captures the surname, given names, date of birth then, following any terminal operator corrections, sends this to the LVH along with the type of ID presented. The LVH must perform an analysis using all the information captured and provide a response to the IST. The responses the LVH provides are as follows:

- The patron has not been detected as being banned.
- The patron has been detected as being subject to an Official Ban applicable to this venue and must be refused entry. The LVH must provide a photo of the banned person (when available) to the IST so that the terminal operator can verify and confirm that a false positive match has not occurred. The ban type along with duration and location must also be displayed to the IST operator. If the terminal operator confirms the match, an email notification to QPS must be made (Refer 3.7.1.14).
- The patron has been detected as being subject to an Official Ban not applicable to this venue. Entry is at the discretion of the venue. The LVH must return the ban type, duration and location(s) the ban is applicable to and provide a photo of the banned person (when available) to the IST so that the terminal operator can verify and confirm that a false positive match has not occurred.
- The patron has been detected as being subject to a Licensee Ban applicable to this venue and should be refused entry. The LVH must return the ban type, duration and provide a photo of the banned person (when available) to the IST so that the terminal operator can verify and confirm that a false positive match has not occurred.
- The patron has been detected as being subject to a Licensee Ban not applicable to this venue. Entry is at the discretion of the venue. The LVH must return the ban type, duration and location(s) the ban is applicable to and provide a photo of the banned person (when available) to the IST so that the terminal operator can verify that a false positive match has not occurred.
- An error has occurred while attempting to perform a Ban Check. In this situation, the terminal operator must attempt to rescan, perform a manual check or try a different IST.

3.5 Identification Scanning Terminal

3.5.1 Software

1. Two-factor authentication must be required to gain access to the system for all user modes (Refer 3.6 Access Control Modes).
2. A logout option must be readily available once logged in to the IST.
3. After a period of 5 minutes has elapsed with no user input, the user must be prompted to remain logged in to the system. Failure to respond to the prompt after 30 seconds must result in the logged in user being logged off the IST.
4. All actions performed on the terminal must be logged at the LVH (Refer 3.9 Logging).
5. Functions offered on the terminal must be restricted based on the group the user is a member of (Refer 3.6 Access Control Modes).
6. The sole use of colour to convey messages, e.g. a patron is or isn't banned, an error has occurred, etc. is not acceptable.
7. Following completion of a Ban Check (Refer 3.4.2 Ban Check Process) the IST display must be cleared of any personal information except for the currently logged in user.
8. The IST must display the following while any user is logged in:
    a. version number of the software
    b. the last date / time the Official Ban list was updated
9. The IST must have the ability to provide a SHA-256 result of the approved software operating on the IST. Identification templates do not need to be included as part of the result.
10. The IST must capture an entry photo of the patron at the time their ID is scanned.
11. The IST must associate the entry photo with the scanned ID details.
12. The IST must transmit the entry photo to the LVH when transmitting the patron scan data.
13. The IST must display a prominent warning message if the Official ban list has not been updated for 5 days. The warning must not impede ban checking and be displayed on the primary screen.
    a. If the Official ban list has not been updated for 10 days, the IST must disable the ability to scan and display a prominent message indicating that scanning has been disabled due to the ban list being out of date. The ability to initiate a ban list update must be presented when in this disabled state.

3.5.2 Identification Scanner

1. The IST must be able to recognise different forms of ID including the following:
    - all Australian Drivers Licenses;
    - all Adult Proof of Age cards and interstate equivalents;
    - Australian and International Passports;
    - Australia Post Keypass Identity card; and
    - foreign drivers licences (must display name, photo and date of birth of the licence holder. Where a foreign driver licence is not written in English, an international driver permit issued in the foreign country of origin (and including a photo of the licence holder and translation) must be presented with the foreign driver licence).

2. The Identification Scanning component of the IST must be able to extract and capture the following information from the above mentioned IDs:
    - Name (i.e. surname and given names)
    - Date of Birth
    - Photo
    - Gender (To be used for reporting purposes only)
3. No other personal information is to be recorded from the scanned ID.
4. The IST must not store or transmit an image of the entire ID.
5. The Identification Scanner component must meet a minimum of 95% scan accuracy under laboratory test conditions. This includes all types of scannable IDs.
6. The IST must perform a check on the date of birth to ensure the patron is at least 18 years of age. A clear indication must be made to the terminal operator if the patron is younger than 18.
7. The IST must have a manual input method for ID that cannot be recognised by the scanner.
8. The IST must perform a check that the ID scanned is not expired.
    a. Where the expiry date cannot be scanned, e.g. when the expiration date is on the back of the ID, a message advising the operator to check the ID for expiration must be made.
    b. Detection of expired ID must not be an auto-refusal of entry as the patron may be carrying adequate evidence that their ID has been renewed, e.g. a receipt from the Department of Main Roads and Transport.

3.5.3 Camera

1. The IST must be fitted with a camera.
2. The camera must be adjustable to accommodate for patrons of varying height.
3. The camera must be capable of taking photos under various lighting conditions.

3.6 Access Control Modes

Access Control Modes are applicable to all ISTs and LVHs. Approved Operators must define their own access control modes for CHs to ensure the security of data held.

3.6.1 Terminal Operator mode

Is used to:

- scan IDs at the point of entry
- verify the scanned result of the ID matches the physical ID and amend any incorrectly scanned data where necessary
- check if the person has been banned
- confirm if a positive Ban Check is accurate

All terminal operator accounts must be set up with:

- The full name of the operator
- A method of logging on to an IST using two-factor authentication

- It is permissible to only require one-factor of authentication when a terminal operator has logged in using two-factors in the last 12 hours at that venue. This is only permissible for users that do not have access to ban lists or patron scan data.

3.6.2 Manager mode

Is used to:

- Create/amend/remove a licensee ban record. This must also include the ability to associate a statement with the data that the patron believes to be inaccurate, out-of-date, incomplete, irrelevant or misleading when the manager determines not to amend the data kept on file
- Add/remove Operators and Managers
- Retrieve and export patron scan data upon request from a law enforcement agency. This must give provision to request date and time periods
- Retrieve and export the current Official Ban list data upon request from a law enforcement agency
- Retrieve and amend a patron's scan data upon request from the patron. This must also include the ability to associate a statement with the data that the patron believes to be inaccurate, out-of-date, incomplete, irrelevant or misleading when the manager determines not to amend the data kept on file
- Request a SHA-256 of the software on the ISS

All Manager accounts must be set up with:

- The full name of the Manager
- A method of logging on using two-factor authentication

3.6.3 Service mode

Is used to:

- Fault find/fix IST/LVH
- Access log file
- Perform IST/LVH software updates
- Request a SHA-256 of the software on the ISS

3.6.4 Administrator mode

Is used to:

- Remotely access the LVH
- Remotely request log files
- Add/remove Managers
- Perform system updates to IST/LVH
- Request a SHA-256 of the software on the ISS

Administrator mode is reserved for the Approved Operator.

3.7 Local Venue Host

Unless otherwise stated, all Local Venue Host requirements are applicable to combined IST/LVH devices.

3.7.1 General

1. Upon power up or an ID scanning session commencement, the LVH should initiate a check of all current ban data with the CH and propagate this data accordingly across venue ID scanner equipment.
2. The LVH must cache patron scan data locally (including the photo taken by the IST) for 30 days (Refer 3.1.5).
3. The LVH must transmit the cached patron records (including the photo taken by the IST) to the CH upon start-up, shutdown and at least every 4 hours. .
4. The LVH must store ban records locally (Refer 3.1.5). Expired bans must be deleted from the LVH.
5. The LVH must have the ability to request from the CH photos which are not currently stored locally.
6. The LVH must refresh (add/remove records) the ban list upon receiving a new list from the CH.
7. The LVH must be capable of processing a request from a Manager to create/amend/remove a Licensee Ban record and forward this to the CH.
8. The information required to create a Licensee Ban record is:
    - Surname
    - Given names
    - Date of Birth
    - Photo
    - Ban duration (start and end date)
    - Ban reason
9. The LVH must add the Venue Name and Precinct to the Licensee Ban record before transmitting to the CH.
10. All data from scanned patron IDs and associated photos captured must be automatically deleted from the LVH after 30 days. The deleted data must be permanently destroyed so that it is no longer retrievable.
11. All actions performed on the LVH must be logged (Refer 3.9 Logging).
12. Functions offered on the LVH must be restricted based on the group the user is a member of (Refer 3.6 Access Control Modes).
13. The LVH must be capable of displaying its version number.
14. The LVH must send a notification to QPS when a positive Ban Check has been made by a terminal operator. The format of the email is:
    - To: pbnappeal@police.qld.gov.au
    - Subject: Contravention of a banning order detected
    - Body: Refer to the data definition table in section 7.3 RPT3 – BANNING MATCH RECORD in the Approved Operators Banning Order Interface Specification

3.7.2 Deleted

3.8 Central Host

3.8.1 General

1. The CH must be able to receive banned person records from OLGR (Refer 3.1.5 and 3.8.3 Banning Order Data File).
2. The CH must be able to receive patron data (including photos captured) and Licensee Ban data from venues (Refer 3.1.5).
3. The CH must be able to propagate Licensee Bans received from LVHs to all other Approved Operators. The method used to exchange data must be securely encrypted and consistent with industry standards. Where a file based exchange is used, the file must be prefixed with the Approved Operators name, or a shortened version.
4. The CH must be able to communicate to all LVHs that are a part of the Approved Operators ISS network the current ban list. Note: The CH does not need to send the photos with every ban list update.
5. The CH must be able to accept a request from LVHs to send a photo of a banned person.
6. When an update to the ban list has been received, the CH has 15 minutes to communicate the ban list to all venues.
7. All data from scanned patron IDs and associated photos captured must be automatically deleted from the CH after 30 days unless a lawful request has been received from a law enforcement agency to retain a specific subset of patron data. The retention of the subset data must not impact on the automatic deletion of unaffected data. The deleted data must be permanently destroyed so that it is no longer retrievable.
8. All patron scan data is to be stored in a form that isn't easily accessible to unauthorised users.
9. The CH must not distribute the patron scan data it received from LVHs to other Approved Operators.
10. The CH must have the ability to reject connections from devices that are no longer trusted (e.g. a device has been stolen).
11. Patron scan data must be retained for 30 days.
12. Deleted
13. Official Bans and Licensee Bans must be removed from the CH once they are no longer in force.
14. Licensee Bans must be exchanged between Approved Operators every 15 minutes.
15. The Central Host must alert the Approved Operator if a new ban list has not been downloaded from OLGR in the last 24 hours.

3.8.2 Central Host to OLGR Data Exchange

1. The CH must be able to connect to OLGR's SFTP server for retrieval of the Banning Order Data File, the current site list and SNOP list and uploading of Approved Operator Data File.
2. Refer to the Approved Operators Banning Order Interface Specification for how to connect to OLGR's SFTP server.
3. Integration testing between the CH and OLGR's SFTP server will be required prior to approval of the CH. The type of testing required will depend on what type of submission is being made I.e. full or update. Refer 6 Contacting OLGR.

4. The CH must check the SFTP server every 15 minutes for an updated Banning Order Data File.

3.8.3 Banning Order Data File

1. The Banning Order Data File residing on the SFTP is in a zip file format.
2. The filename of the Banning Order Data File is “ban_list_[yyyymmddhhmmss].zip”.
3. Associated with this zip file will be a SHA-256 file of the Banning Order Data File named “ban_list_[yyyymmddhhmmss].sha256”.
4. The contents of the zip file will include the following:
   - The Official Ban list in XML format named “ban_list_[yyyymmddhhmmss].xml”
   - Photos of banned persons named “[1234567890].[extension]”.
5. The file type of the provided banned persons photos will be one of the following:
   - JPEG
   - BMP
   - PNG
6. The Official Ban list XML file will conform to OLGR’s XML Schema Definition. This can be provided upon request. Refer to the data definition table in section 7.1 RPT1 – QPS BANNING ORDER DATA FILE in the Approved Operators Banning Order Interface Specification.

3.8.4 Approved Operator Data File

1. The Approved Operator Data File must be uploaded to the OLGR Data Centre by 9am every day.
2. The Approved Operator Data File must be in a zip file format.
3. The filename of the Approved Operator Data File must be named “ao[99]_[yyyymmdd].zip”. Where [99] is the number assigned to the Approved Operator by OLGR and [yyyymmdd] is the date the file is uploaded.
4. The Approved Operator Data File must contain the following:
   - The Scanning Report CSV File
   - Daily CSV Log File
   - Approved Operator CSV Log File
5. The filename of the Scanning Report CSV File must be named “scanning_report_ao[99]_[yyyymmdd].csv”. Where [99] is the number assigned to the Approved Operator by OLGR and [yyyymmdd] is the date the file is uploaded to OLGR. Refer to the data definition table in section 7.4 RPT4 – DAILY SCANNING REPORT in the Approved Operators Banning Order Interface Specification.
6. The filename of the Daily CSV Log File must be named “log_ao[99]_site_[yyyymmdd].csv”. Where [99] is the number assigned to the Approved Operator by OLGR and [yyyymmdd] is the date the file is uploaded to the CH.
7. The filename of the Approved Operator CSV Log File must be named “log_ao[99]_[yyyymmdd].csv”. Where [99] is the number assigned to the Approved Operator by OLGR and [yyyymmdd] is the date the file is uploaded to the OLGR.
8. Associated with this zip file will be a SHA-256 file of the Approved Operator Data File named “ao[99]_[yyyymmdd].sha256”.

3.8.5 Current Licensed Premises List

Refer to the data definition table in section 7.2 RPT2 – CURRENT LICENSED PREMISES LIST in the Approved Operators Banning Order Interface Specification.

3.9 Logging

3.9.1 General

1. A log file must be maintained by an IST, LVH and CH.
2. The log files residing on the IST and LVH must not store any information that can identify patrons.
3. ISTs and LVHs are required to upload their log files to the CH upon start-up, shutdown and at least every 4 hours.
4. The log file must be in CSV format.
5. The log file must be maintained for a minimum period of 90 days.
6. The system clock of each logging source must be synched to a common time source.
7. IST, LVH and CH log files must be provided to OLGR prior to being purged.

3.9.2 Log File Format

1. Each entry in the log file must follow a consistent and acceptable format with the following details. Refer to the data definition tables in section 7.5. RPT5 – DAILY LOG FILE REPORT (IST AND LVH LEVEL) and section 7.6 RPT6 - DAILY LOG FILE REPORT (CH LEVEL) in the Approved Operators Banning Order Interface Specification:
   - Site Number
   - Date Time
   - Device Identification Number
   - Username
   - User Mode
   - Action (Refer 3.9.2.2)
   - Details of action
2. The following is a list of the Action Codes and their associated Actions for identifying ‘Management Activities’ performed by an ID Scanning Terminal:
   a. User log on
   b. User log off (user initiated or time-out)
   c. ID recorded on LVH (on successful ID check)
   d. ID recorded on LVH (with operator modifications)
   e. Communication Failures
   f. Hardware Failures e.g. scanner failure
   g. Positive Ban Check (confirmed by terminal operator)
   h. False Positive Ban Check (terminal operator dismisses potential ban match i.e. photos do not match)

i. Request from LVH for ban person details (LVH only) – This should only be recorded when the LVH polls the CH for an updated ban list

j. Received ban person details (LVH only) – This should only be recorded in response to a request from the LVH for ban person details. Note, this is separate from l.

k. ID recorded on CH

l. Ban records updated from CH (LVH only) – Refer 3.8.1.6

m. Licensee Ban record created (LVH only) – This is recorded when the ban is first created. This should not be recorded when it is propagated to other LVHs.

n. Licensee Ban record amended (Manager Mode) – This is recorded when an amendment is manually made. This should not be recorded when it is propagated to other LVHs.

o. Licensee Ban record deleted (Manager Mode) – This is recorded when a Licensee Ban is manually deleted. This should not be recorded when it is propagated to other LVHs or expires.

p. User created (include username and access controls) (LVH only)

q. User access mode changed (include former access control and new access control mode)

r. Intrusion detection event

s. Failed log on

t. Remote connection

u. Changes to access controls

v. Software updates

w. Service start up

x. Service shutdown

y. Deleted

z. Patron data retrieved (Manager mode) – This should only be logged when personal details are accessed. Viewing a photo only does not require this code to be recorded.

aa. Patron data exported (Manager mode)

bb. Patron data amended (Manager Mode)

cc. Patron data removed (30 day expiry)

dd. Updated official ban list received from OLGR (CH only) – Details of action must begin with the filename and extension of the ban list downloaded. Additional information may also be recorded. E.g. ban_list_20170701073015.zip downloaded – XX ban processed.

ee. Updated licensee ban list received from AO (CH only) - Details of action must begin with the filename and extension of the ban list downloaded. Additional information may also be recorded. E.g. Acme_ban_list_20170701073015.zip downloaded – XX ban processed.

ff. Failed to download ban list (CH only)

3.10 ID Scanner Management Reporting

3.10.1 General

1. Non personal data is required to be sent to permit research, analysis and evaluation of the effectiveness of the ID Scanner initiative.
2. The data is to be provided in a secure manner.
3. Other ad-hoc reports may also be requested to be supplied to assist with the evaluation process.

3.10.2 Deleted

3.11 Physical Security

1. Any venue based ID scanner equipment that contains confidential data must be secured via one or more seals. Refer to OLGR Approved Seals.
2. Access to the interior of such equipment must only be possible by breaking a seal. Particular attention must be given to PC based LVHs for this requirement. Often easy access can be obtained by removing spare drive bay covers, or by unscrewing the power supply, or removing other panels.
3. Exposed ports must be electrically disconnected or capped with an approved method if not in use to prevent unauthorised access. Disablement of ports via firmware may also be considered acceptable if it can be proven that the firmware is sufficiently locked down.

4 Manual Ban List

4.1 Purpose

Section 173EJB of the Liquor Act 1992 (Liquor Act) provides that in the case of an ID scanning system failure, the approved operator must ensure the licensee has immediate access to a current list of persons who are subject to a banning order for the premises. This section details the information required to be provided on the manual ban list.

While this section does not prescribe the method of how the manual ban list is to be distributed, only offering a single way of retrieving this list, which itself could be subject to failure, would unlikely be considered to meet the intent of s173EJB.

4.2 Ban List Format

1. The following information must be contained on each page of the manual ban list:
   - Clear title distinguishing the list as the manual ban list (as to avoid confusion with the full official ban list export. Refer 3.6.2).
   - The venue name the list has been generated for.
   - The precinct name the venue is located in.
   - The Approved Operator name.
   - The date the ban list was generated.
   - The date the ban list expires (a manual ban list remains current for 7 days from when it is generated).
   - Page number and total number of pages in the list i.e. page 2 of 3.
2. The manual ban list must only contain official bans for the regulated premises that it is generated for.
3. Banned person information must be sorted alphabetically by surname and presented in a manner that is suitable for use.
4. The following information must be provided on the manual ban list for each person who is banned:
   - Surname
   - Given names
   - Date of birth
   - PersonID
   - Photo (where available)
   - NicheID (where multiple exist, use the nicheID that corresponds to the latest expiration applicable to the venue that the list is generated for must be used)
   - Ban expiration (where multiple exist, the latest expiration applicable to the venue that the list is generated for must be used)

5 Submission Requirements

5.1 General

1. All submissions to OLGR must contain a letter that formally requests OLGR to perform an evaluation of the product being submitted. This letter must contain at least the following elements:
   - The date of the submission.
   - All letters must be addressed to the Executive Director, OLGR and marked ATTN: Technical Unit.
   - A description of the product/s being submitted and the intent of the submission. This may be in tabular form if there is more than one item being submitted.
   - The name and signature of the person/s responsible for the submission and contact details of where technical enquires regarding the submission may be directed.
2. All submissions to OLGR must contain a "Certification and Indemnity Form" which is signed by a person of an acceptable level to the OLGR Executive Director. For example, the CEO or compliance manager of the company would be acceptable or an officer who can be held accountable for the submission (if it is unclear whether or not the person is of an acceptable level, OLGR should be contacted). A copy of this form may be found in Appendix I. This form must reference the version of the system/software/hardware that is being submitted.
3. All submission documents and software must be submitted in an IBM PC compatible electronic format. Note that if proprietary software is required in order to open, view or otherwise interpret information, this software may need to be supplied by the submitter.
4. All submissions including comments in source code must be in English.
5. Where appropriate, submissions must contain a point by point response to the applicable minimum requirements in this document and other relevant OLGR technical requirements document(s).
6. To assist in the evaluation of a submission, a report of any testing conducted on the product (prior to the submission) should be submitted. This report must contain the testing body's name, the name of the individual who conducted the testing, a description of what was tested, how it was tested (photos may be required) and the test results.
7. If the submission is an update submission, then the submission must include a complete list and description of all the changes.
8. All submission documentation and electronic media must be labelled with the company name, the product name, the product version and the submission date. Resubmissions must also include the resubmission number, e.g. version 2. Note: version numbers are to be unique and any change to an already approved submission should require this unique version number to change.
9. All submissions must include a list of all known unresolved issues, bugs and incidents. This list must be comprehensive and include any issues identified with previous versions which have not been resolved with the current version, even if these issues have been previously notified to OLGR. Note: submissions are "evaluation type" specific, so if the submission is relating to a particular product or system component then it is expected that the list of all known unresolved issues, bugs and incidents is related to that particular product or system component (rather than the entire system overall).

5.2 Hardware Submissions

1. Depending on the applicable legislation or requirements, a hardware sample of the product may be required in order to complete an evaluation of a product. If it is unclear whether or not a hardware sample is required for a submission, OLGR should be contacted. Note: that this does not initially have to be a final production version (the version that will be actually used), but a final production version will be required at some stage in order to complete the evaluation.
2. Hardware submissions must contain a Part / Model Name, Part / Model Number and the date of manufacture of the item itself.
3. Hardware submissions must contain any equipment that may be required in order to perform an evaluation. For example, specialised software, custom tools, keys, test harnesses, etc.
4. Hardware submissions must contain all standard maintenance tools sold with the equipment.
5. Hardware submissions must contain applicable user / operational manuals, service manuals and installation manuals.
6. Hardware submissions must contain a statement signed by a person of an acceptable level to the Executive Director, which states that all hardware submitted has been previously tested as being electrically safe, and meets all other statutory obligations with regard to electrical and other safety.
7. Hardware submissions must contain all notes and warnings with regard to the safe use of the product. For example, cautions and warnings with respect to potential electrical shock hazards must be included in the submission.
8. Hardware submissions must contain a detailed list of the functions of all control elements (such as switches, dials, dip switches, jumpers, etc.).
9. Technical documents (such as technical drawings, circuit diagrams, PCB layouts, schematics, photos, data sheets, etc.) may be required for certain types of hardware submissions.
10. The results of electromagnetic, electrostatic and radio frequency interference testing may be required for certain types of hardware submissions.

5.3 Software Submissions

1. Depending on the applicable legislation or requirements, software may be required in order to complete an evaluation of a product. If it is unclear whether or not software is required for a submission, OLGR should be contacted. This section is applicable to all software submissions.
2. When required to submit software, the following applies:
    a. If the software is publicly available (i.e. it is “off the shelf”) supply the software name and version number. Depending on the type of submission, a copy of the software may be required.
    b. If the software is proprietary and developed by the submitter, or “sub-contractor” acting on behalf of the submitter, then the source code is required (Refer 5.4 Source Code Submissions).
    c. All executables submitted must have SHA-256 hash values stated on the signed submission letter. If there are many executables then a combined hash result (SHA-256 of a manifest file) is acceptable as long as a broken down list is supplied electronically elsewhere with the submission.
    d. All software submitted must have the facility to perform SHA-256 over all regulated ISS component files intended for the production system or where applicable, the software should be digitally signed. Where possible this facility should have the

ability to specify a single file or create a combined hash result (SHA-256 of a manifest file) of all regulated ISS component files.

3. Depending on the type of the software being submitted, and on the number of changes from previously approved software, program block diagrams, flow charts and other information that describes the software algorithm may be required. Note that this information will always be required for submissions of new software.
4. If the software being supplied has been previously evaluated (i.e. the submission is an update to a previously approved version), supply a complete and comprehensive change / revision history. This should include as a minimum, a list of the individual module / file names with corresponding changes and this also must include the reason for the change.
5. Submissions of software updates must include the entire software, and not just the modules that have been modified.

5.4 Source Code Submissions

1. As per section 5.3, source code may be required to be submitted. Generally, a source code submission will require the source code, a compiler, assembler, linker and any other tools that are required to compile the final executable files (or binaries if applicable). OLGR should be contacted to determine exactly what is required to be submitted (Refer 6 Contacting OLGR). This section is applicable to all source code submissions.
2. Where required, any source code submitted must be complete and able to be compiled. Compiled binary / executable files must also be supplied.
3. All compiled binary / executable files required to operate / run the equipment must be supplied.
4. OLGR must be able to compile the submitted source code. This is to ensure that the output of the compilation of submitted source code is identical to submitted precompiled code in order to allow verification of source code with object code. This may require supplying OLGR with a licensed copy of the compiler, linker, assembler etc. and in some circumstances, a PC to perform the compilation (e.g. a LINUX PC may be needed to compile the source code).
5. Source code submissions must contain detailed, step by step instructions on how to setup, configure and use the compilation program(s) to create the binary / executable files. In addition, these submissions must provide software versions with respective SHA-256 for each binary / executable file for verification purposes.
6. All source code is to be properly commented and contain a change/revision history. If applicable, module descriptions or similar should also be supplied.

6 Contacting OLGR

Before making a submission, it is recommended that OLGR be contacted well in advance, so that the product can be discussed, submission requirements ascertained and evaluation resources planned.

In this regard, the Manager Gaming Services (Technical), OLGR should be contacted on telephone (07) 3872 0828 or email olgrnotify@justice.qld.gov.au.

7 Revision History

Version	Changes	Release Date	Inception Date
1.0	• Initial release for industry and other stakeholder comment	07/08/2014	30/04/2014
1.1	• Updated to incorporate feedback from release 1.0	15/09/2014	15/09/2014
1.2	• Changed URL on page 2 from www.olgr.qld.gov.au to https://www.business.qld.gov.au/industry/liquor-gaming • Updated 3.1.1 to reflect the position to be taken with value added services • DJAG template update	05/03/2015	05/03/2015
1.2.1	• DJAG template update	12/04/2016	12/04/2016
1.3	• Added SHA-256 to glossary • Changed from SHA-1 to SHA-256 for Banning Order Data File	24/01/2017	24/01/2017
1.4	• Removed reference to Queensland Government Statistician's Office (3.10.2) • Removed reference to SNOS (2.1 & 3.10.1.1) • Removed appendices II-V and instead refer to these being in the Approved Operators Banning Order Interface Specification • Updated sections 3.8.3 and 3.8.4 to be consistent with Approved Operators Banning Order Interface Specification v2 • Minor grammatical fixes	03/03/2017	03/03/2017

Version	Changes	Release Date	Inception Date
1.5 Draft	• Added 3.4.1.5 (Partial matching) • Added 3.5.1.13 (Ban list expiry) • Added 3.5.2.8 (Expired ID) • Added 3.8.1.13 (Expired bans) • Added 3.8.1.15 (Ban list download alert) • Added 3.8.5 (Site file) • Added 3.9.2.2.ee (Licensee ban download) • Added 3.9.2.2.ff (Failed download of ban list) • Added 3.11 (Physical security) • Added 4 (Manual ban list) • Updated 2.5 • Updated 3.3.3 (Firewall whitelist) • Updated 3.4.1.1 (Ban check process) • Updated 3.4.1.5 (Partial matching) • Updated 3.4.2 (Ban check analysis) • Updated 3.5.1.3 (IST timeout) • Updated 3.5.1.9 (SHA-256, templates) • Updated 3.6.1 (2FA) • Updated 3.6.2 (SHA-256, add 2FA to LVH) • Updated 3.6.3 (SHA-256) • Updated 3.6.4 (SHA-256) • Updated 3.7 (Clarification for combined IST/LVH) • Updated 3.7.1.3 (Upload frequency) • Updated 3.7.1.4 (Expired bans) • Updated 3.7.1.14 (QPS email) • Updated 3.8.1.3 (Licensee ban file name) • Updated 3.8.1.14 (Licensee ban list frequency) • Updated 3.8.2.1 (Site file) • Updated 3.8.2.3 (Integration testing) • Updated 3.8.2.4 (Official ban list frequency) • Updated 3.8.4.4 (Daily log file) • Updated 3.8.4.6 (Daily log file) • Updated 3.9.1.3 (Log frequency) • Updated 3.9.2.2 (Log file action clarifications) • Updated 3.9.2.2.dd (Official ban download) • Updated 3.11.3 (Capping) • Updated 4.3.2 (SHA-256) • Updated 4.4.5 (SHA-256) • Updated 5.3.2.d (Regulated files) • Updated further reading • Deleted 3.7.2 (Physical security) • Deleted 3.8.1.12 (Site file) • Minor grammatical fixes	18/08/2017	
1.5 Final	• Updated 3.5.1.13 (Ban list expiry) • Updated 3.6.1 (2FA) • Updated 3.8.4.6 (Daily log file) • Updated 3.6.2 (2FA)	09/10/2017	30/11/2017

Appendix I

Certification and Indemnity Form

I _____(Full Name)

being _____(Position Held)

for and on behalf of _____

_____(Supplier)

1. warrant that the Supplier has obtained (or will obtain prior to implementation) and will maintain all licences, approvals, consents, permissions and assignments necessary to perform the actions or carry out the activities in respect of which this application or its subsequent approval relates without infringing the intellectual property rights of any third parties;
2. indemnify the State of Queensland, the Chief Executive Officer, Office of Liquor and Gaming Regulation and their officers, employees and agents ('those indemnified') from and against any actions, proceedings, claims, demands, costs (including all reasonable legal costs and all reasonable costs associated with defending those indemnified), losses, damages and expenses, including those arising out of the terms of any settlement, which:
    a. may be brought against or made upon those indemnified; or
    b. those indemnified may occur or sustain,

    arising out of or as a consequence of any official act undertaken by those indemnified when acting within the scope of their duties and responsibilities, regarding this application or any subsequent approval, whether in relation to the alleged infringement of the intellectual property rights of any third parties or otherwise;
3. certify that the statements contained in the attached documents are to the best of my knowledge and belief true and correct in every detail and are a complete disclosure of the information requested; and
4. certify that the items submitted are complete and operational.

Name/Description of Equipment _____

signed at _____

This _____ day of _____ 20 _____

_____
(signature of Deponent)

in the presence of _____
(signature of Witness)

Name and Address of Witness _____

_____

_____