Liquor & Gaming NSW

Code of Practice: Facial Recognition Technology in Hotels & Clubs

16 March 2026

www.liquorandgaming.nsw.gov.au

NSW GOVERNMENT

Table of Contents

Foreword 1
Background 2
Self-exclusion and facial recognition technology 2
One-to-one versus one-to-many 2
Regulatory framework 3
Requirements for the installation and operation of facial recognition technology in venues in NSW 5
1. Privacy impact assessment and data breach response plan 5
2. Installation and controls 6
3. Signage 7
4. Data storage 7
5. Data access and use 8
6. System performance and integrity 9
7. Venue staff response to positive matches 10
Attachment A – Checklist of technical and operational requirements for FRT providers i

Foreword

The NSW Government committed to a series of reforms to minimise gambling harm and prevent money laundering in hotels and clubs. This includes introducing a statewide exclusion register that is supported by facial recognition technology (FRT) in all venues with gaming machines.

This Code of Practice (the Code) has been developed to provide guidance to hotels and clubs (venues) on the appropriate use of FRT to identify patrons who have excluded themselves from venues or areas in venues with gaming machines. Venues should seek independent legal advice to ensure their use of FRT complies with their legal obligations as they relate to their individual circumstances.

The requirements in this Code apply to venues currently operating FRT or that choose to install FRT prior to its use being mandated. The Code will remain in effect until any future legislative change to mandate FRT.

The NSW Government has committed to mandating FRT and to integrate this with the future state-wide exclusion register. Compliance with this Code will help venues and FRT providers prepare for the introduction of the statewide register and associated FRT requirements, which will supersede the Code, upon commencement.

The Code applies to the use of FRT in venues primarily in relation to enforcing exclusion orders. The use of FRT for anti-money laundering (AML) purposes will be addressed in future reforms.

FRT providers are not required to seek Government approval to install and operate FRT in venues under this Code. Rather, it will be up to venues to supply FRT providers with the attached checklist of technical and operational specifications (**Attachment A**). It is strongly recommended that venues also require their FRT provider to complete the attached statutory declaration that the technology installed in the venue meets the specifications.

The Code has been approved by the Minister for Gaming and Racing under Division 3, Section 48 of the *Gaming Machines Act 2001* (the Act). The Code is to take effect on the day that it is published in the NSW Government Gazette.

Venues cannot be penalised for contravening the Code under the Act. However, the NSW Government encourages all venues to ensure they are compliant with the Code and best practice use of FRT. Accordingly, use of the terms ‘requirement’ and ‘must’ in the Code relate to standards that venues are expected to meet in order to be compliant with the Code, not necessarily what is mandated by legislation.

Venues that have FRT installed are expected to take steps, without delay, to ensure their system is compliant with the Code. Where significant upgrades to existing systems are needed to meet one or more requirements, the expectation is that venues will become Code compliant within 6 months of its commencement.

Liquor & Gaming NSW is committed to working with industry to help ensure that both existing and future FRT and exclusion registers comply with the Code.

The Liquor & Gaming NSW Hospitality Concierge is available to provide further information to industry to meet its requirements and to answer any questions about the Code. A contact form for the Hospitality Concierge can be found here.

Background

Self-exclusion and facial recognition technology

Self-exclusion is an important harm minimisation measure where a venue patron experiencing significant gambling harm can sign an agreement to be excluded from one or more venues or areas of those venues for an agreed period, from six months to indefinitely.

Currently, the patron provides a photograph which is displayed in an area or kept in a digital or hard copy folder accessible only to venue staff and is used to identify the patron. Following a positive identification of a self-excluded patron, a staff member will approach the patron to discuss the self-exclusion and invite the patron to leave the premises or venue area.

A known limitation of this process is the utilisation of manual detection methods where the identification of a self-excluded patron largely relies on the eyesight and memory of venue staff. This can lead to higher than acceptable 'breaches' of standard self-exclusion agreements and reduced effectiveness of the program.

Integration of facial recognition technology with self-exclusion enables an automated process of identifying patrons who have self-excluded from a venue. This is more accurate and reliable compared to manual methods. Automated detection methods are particularly useful for monitoring and identifying excluded patrons in crowded venue environments, which can be challenging for busy venue staff.

Facial recognition technology is a computer system or device capable of matching the features of a human face based on a live image against an existing image from a digital database.

A facial recognition system will generally consist of:

- a fixed video capturing device/s (FVCDs), i.e. a camera
- proprietary software which uses complex algorithm(s) to analyse digital facial images captured by FVCD(s) to extract unique facial features and mathematically encode them into a biometric template, comprised of a numerical vector.[1]
- a graphical user interface (GUI) to view and manage the capturing of images for the purpose of identification
- a data storage system hosted on-premises, in the cloud, or a hybrid of both.

Venues are currently using FRT together with existing ClubSafe and BetSafe exclusion registers or individual club sign-in systems to manage exclusions more effectively.

This Code is intended to support venues already operating FRT and those wanting to install FRT to support the ethical and responsible application of the technology and to improve the ability of venues to detect excluded patrons.

One-to-one versus one-to-many

There are two main ways FRT is deployed:

[1] Note. This process enables FRT systems to compare and match faces with an existing database.

- **One-to-one** FRT is used to verify the identity of an individual by checking a captured image against a single recorded image to determine if both images are the same person. A common application of one-to-one FRT is to unlock a smartphone.
- **One-to-many** FRT is used to identify an individual by comparing a captured image against a large database of recorded images. A common use of one-to-many FRT is to identify a person in a crowd for surveillance and law enforcement. One-to-many FRT is notably more prone to error as it typically operates in uncontrolled environments. It also has greater privacy implications compared to one-to-one FRT.

The use of FRT in venues most closely aligns to the one-to-many approach. The database against which patron images are compared, however, is confined to a relatively small cohort of excluded individuals. Nevertheless, the principles and requirements in this Code are based on the characteristics of one-to-many FRT.

Regulatory framework

The following key legislation is relevant to the use of FRT in venues with gaming machines in NSW.

Gaming Machines Act 2001

Under Section 49 of the Act, a venue with Electronic Gaming Machines (EGMs) must ensure patrons have access to a self-exclusion scheme and must publicise the availability of self-exclusion schemes and information about how they operate to the patrons of the venue.

It is lawful under the Act for venue staff to prevent excluded patrons from entering or to remove excluded patrons from the nominated area of the venue, using no more force than is reasonable in the circumstances.

No legal action can be taken against venue staff for any act done or omitted in good faith with respect to an excluded patron, or if an excluded patron enters or remains in the nominated area of the venue.

Gaming Machines Regulation 2019

Clause 45 of the Regulation provides the minimum requirements for the establishment and conduct of self-exclusion schemes including, among other requirements, that the venue must ensure that participants in the scheme can be readily identified, whether by means of access to a recent photograph of the participant *or otherwise.*

FRT strengthens the capacity for a venue to identify participants in the scheme and to remove or to cause that patron to be removed from the nominated area of the venue.

The Privacy Act 1988

There are 13 Australian Privacy Principles (APPs) under the Privacy Act that govern standards around the collection, use and disclosure of personal information. To breach any of these APPs is to 'interfere with the privacy of an individual' and can lead to regulatory action and penalties.

Australian Privacy Principles:

- Open and transparent management of personal information
- Anonymity and pseudonymity
- Collection of solicited personal information
- Dealing with unsolicited personal information

- Notification of the collection of personal information
- Use or disclosure of personal information
- Direct marketing
- Cross-border disclosure of personal information
- Adoption, use or disclosure of government related identifiers
- Quality of personal information
- Security of personal information
- Access to personal information
- Correction of personal information

Facial biometric information is considered sensitive information under the Act which is generally afforded a higher level of privacy protection under the APPs than other personal information. The individual about whom the sensitive information relates must consent to its collection unless an exception applies.

The Act and its APPs automatically apply to organisations with an annual turnover of more than $3 million. Organisations with annual turnover of $3 million or less may also opt-in to the Privacy Act, which is strongly recommended under this Code (see requirements section below). Accordingly, FRT providers and venues operating FRT should be considered 'APP Entities' under the Act.

The Code has been developed with consideration of its alignment to the APPs and therefore compliance with this Code will help support venues in meeting their obligations under the Privacy Act. Through compliance with the Code, venues also make a public commitment to ethical and responsible use of FRT and will benefit from any resulting increase in patrons' confidence and trust.

However, it is important to note that the Australian Information and Privacy Commission may at any time exercise its regulatory power to investigate and take enforcement action in relation to a venue or FRT provider's compliance with the APPs. This is irrespective of a venue or FRT provider's compliance with the Code.

More information about the Commonwealth Privacy requirements can be found at the Office of the Australian Information Commissioner website: www.oaic.gov.au

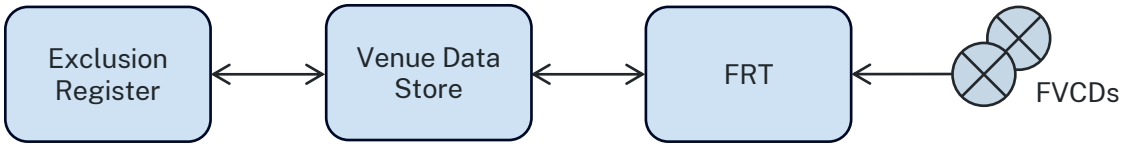
Requirements for the installation and operation of facial recognition technology in venues in NSW

For use in venues in NSW, FRT must be capable of identifying or verifying the physical features of an excluded patron's face using a digital image captured from a fixed video source.

At a high level, the system must be able to:

- communicate securely with an exclusion register or a venue's patron data store
- use exclusion data to compare with the images of persons entering a venue or gaming area
- send a notification to an authorised person at the venue when a suspected excluded person is identified
- prevent unauthorised access, use and disclosure of any data collected.

The diagram below shows the basic components of FRT in venues with interactions between these components and information flows signified by arrow lines.



This section contains FRT requirements with which the venue is expected to comply. A separate compliance checklist and a strongly recommended declaration form, including technical system and operating requirements, has been developed at **Attachment A** for venues to supply to their FRT provider. The venue should collect and retain a signed copy of the statutory declaration.

1. Privacy impact assessment and data breach response plan

The following requirements aim to ensure the privacy risks associated with FRT are proactively identified and that strategies are set out to manage, minimise or eliminate those risks.

1.1 The venue should be treated as an "APP Entity" under the *Privacy Act 1988*. As such, it is strongly recommended that venues with an annual turnover of $3 million or less 'opt in' with the Office of the Australian Information Commissioner at https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/opting-in-to-the-privacy-act.

1.2 The venue must collaborate with their FRT provider and/or legal advisor to complete a Privacy Impact Assessment (PIA) on the use of the specific FRT product in the venue prior to the installation of any technology.[2] Where a FRT provider has completed a PIA previously or an industry-wide PIA template is available, the existing report may be re-purposed with the necessary amendments to fulfil this requirement. Completed PIAs must be retained by the venue and provided to Liquor & Gaming NSW on request. The Office of the Australian

[2] Venues with existing FRT installed, that have not completed a PIA, may do so retrospectively.

Information Commissioner provides guidance on how to conduct a PIA here - Privacy impact assessment tool.

1.3 Once installed, venues must update their privacy policy as soon as practicable to reflect the use of FRT in the venue. Liquor & Gaming NSW will provide suggested wording for venues to adopt. Where applicable, venues should update other signage and/or communications to notify their patrons of FRT use, this may include (but is not limited to) venue 'Conditions of Entry' signage, membership applications and/or venue websites (including the privacy policy webpage).

1.4 The venue must collaborate with their FRT provider to complete a response plan that sets out procedures and clear lines of authority in the event of a suspected or confirmed data breach. If the venue has an existing data breach response plan for its digital storage practices in general, this plan can be updated to incorporate processes for responding to FRT-related breaches. The Office of the Australian Information Commissioner provides guidance on how to prepare a data breach response plan. In the event of a data breach, the Australian Information Commissioner and individuals and organisations affected by the incident must be notified in line with the requirements under Part IIIC of the Privacy Act. The venue must also notify Liquor & Gaming NSW as soon as practicable.

2. Installation and controls

The following is a list of requirements that must be adhered to when installing FRT in venues.

2.1 FRT must be installed by persons holding the appropriate trade credentials to perform this type of work. In NSW, a Class 2 security licence is required to sell, install, maintain and repair security equipment (more information here). Key identification and trade credentials of FRT installers, including installer name, date of installation and installer licence number must be recorded in the venue FRT change management log (see also requirement 2.8).

2.2 The venue must have a secure, high-speed, and reliable internet connection. The *Telecommunications Act 1997* sets out rules for Statutory Internet Providers to ensure that all premises around Australia can connect to fast networks, including peak download and upload speeds of at least 25/5 Mbps.[3] Venues are permitted to continue use FRT offline, during an unplanned disruption to service for a maximum of 48 hours, whilst awaiting for restoration of internet service.[4]

2.3 In consultation with the FRT provider, the venue must determine the appropriate number and positioning of cameras to provide the best opportunity to capture the front facial profile of all patrons entering the venue or gaming areas (see **Attachment A** for technical considerations).

2.4 Venues must not link their FRT system to any other venue software that stores biographical data including venue sign-in databases, scanned credentials, or payment mechanism, to preserve patron anonymity.

2.5 Monitors, tablets, or other screen devices used to display images of excluded patrons to authorised staff must neither be accessible nor visible to other staff, patrons or members of the public. This includes if a venue continues to use paper/hardcopy images of excluded patrons.

2.6 The venue's internal control procedures should include measures to ensure such devices cannot be inadvertently picked up, accessed, or viewed by unauthorised persons. This includes ensuring that authorised staff always keep handheld devices on their person while on duty,

[3] The Code recognises that fast, reliable Internet networks may be less available for venues in remote locations which may require case-by-case consideration of alternative Internet options.
[4] Venues should notify their exclusion register operator (where applicable) as soon as soon as practicable of any disruptions to internet service and when service has been restored.

fixed monitors are located where authorised staff are consistently present, and consideration of the physical security of devices, including during non-trading hours.

2.7 The venue must ensure that a current onsite service and hardware replacement agreement is in place to facilitate a rapid response in the event of hardware failure. The agreement should stipulate that a technician is always available during venue trading hours and response. The agreement should also note that repairs will be completed as soon as practicable, considering the system diagnosis and relevant external factors[5].

2.8 The venue must retain detailed installation documents, including FRT hardware and software specifications, configurations and settings, and maintain a change management log describing any significant modifications to the system (which must be kept separate to the Gambling Incident Register) (refer to **Attachment A** for the FRT provider's responsibility to notify the venue of software and hardware updates). The venue must provide these documents to Liquor & Gaming NSW on request.

3. Signage

3.1 Venues must install FRT signage provided by Liquor & Gaming NSW. This signage will ensure that all patrons, excluded and non-excluded alike, are made aware that FRT is being used in the venue, and by entering the venue, give their consent for the FRT to scan and analyse their biometric features.

The following requirements relate to the signage size and display.

3.2 The signage must be displayed where it is clearly visible to patrons and in a way that brings attention to the use of FRT in the venue. It should be displayed in the areas where facial recognition is being used, for example, the entrance to the gaming area or the entrance to venue or both.

3.3 Printed signage must be displayed according to the original dimensions, i.e., printed signs cannot be enlarged or reduced in size.

3.4 For electronic signs, screen display size must be at least 21.5" measured diagonally, and images must be displayed in high resolution and maintain the original aspect ratio. Electronic signs must always be visible, i.e., not part of a rolling display.

More detailed requirements for printed and digital signs can be found on the Liquor & Gaming NSW Website.

4. Data storage

The following is a list of requirements to facilitate the secure storage of patron data necessary to operate FRT in venues in NSW. If uncertain of any data storage requirements, venues should liaise with their IT or FRT provider to confirm they are compliant.

4.1 Data storage linked to the FRT system must remain exclusively in Australia and cannot be exported off-shore, regardless of whether the venue uses an on-premises or cloud-based solution. On-premise servers must be securely stored under lock and key and not accessible to unauthorised staff or the public. This may include storage in a locked room or area and/or access secured through use of keys or security codes.

[5] The Code recognises that same-day services may be less practicable in regional and remote locations and will require case-by-case consideration of a more suitable timeframe.

4.2 The venue must store excluded patron data in a separate location to other venue data. This separate data store must be firewall protected and encrypted (see **Attachment A** for the minimum technical standards).

4.3 The venue must only store the minimum necessary information to identify and assist an excluded patron, including the patron's image, their name or a unique identifier, the start and end date of their exclusion, and area/s of the venue from which they are excluded.

4.4 Information about a previously excluded patron must be deleted from the venue's data store (excluding any incidents recorded in the Gambling Incident Register) as soon as practicable following expiry or revocation of the self-exclusion. Automated notification or deletion mechanisms should be established to support this requirement.

4.5 The venue's data store must incorporate data backup and recovery measures to ensure that critical information about excluded patrons can be restored in the event of data loss or corruption.

4.6 Data relating to system usage, performance, and maintenance reports must not include identifiable patron information and must be retained for a minimum of three years.

5. Data access and use

The following is a list of requirements for managing access to secure FRT data and ensuring the use of FRT is consistent with its primary purpose.

5.1 The venue must have documented control processes for authorising staff to access the user interface, including procedures for onboarding and training staff with specific roles in the system and immediate removal of authorised users who exit their role. The venue must keep a record of staff that have been trained for at least 5 years.

5.2 If the FRT requires the venue to transfer information from an existing exclusion register to their own data store, this must only be completed by an authorised user, either within the same day or as soon as practicable from when they are notified of the patron's exclusion.

5.3 The venue must ensure that excluded patrons have given express consent for certain biometric information to be used to support their identification in the event of an exclusion breach.[6] The venue must also keep a record of excluded patrons' consent relating to the use of FRT.

5.4 FRT must primarily be used for the purpose of enforcing gambling-related exclusions. FRT may also be used for compliance with other regulatory obligations, including liquor banning orders or financial crime-related exclusions.

5.5 The use of FRT, including excluded patron's personal and biometric information, for any commercial or marketing application, or to track patrons for other non-regulatory purposes, is strictly prohibited. This cannot be negated by obtaining a patron's express consent. However, non-identifiable usage data may be used for the purpose of evaluating and improving system performance or to support public health research or policy development.

5.6 The venue must not use information provided by a previously excluded patron for the purpose of contacting them to encourage their return to the venue and/or to gamble. This includes, but is not limited to, sending any communications or marketing that promote gambling.

[6] Amendments to the current self-exclusion agreement terms are required to ensure patrons' express consent is obtained at sign-up. Where practicable, notification must also be sent to patrons already on an exclusion register informing them of these amendments and to provide them with an opportunity to contact the venue or self-exclusion register with any concerns. To avoid duplication, notifications will need to be facilitated by the BetSafe and ClubSafe register operators for member venues, while non-member venues must be responsible for sending their own notifications. Liquor & Gaming NSW will provide support in relation to these amendments, including suggested wording for changes to the self-exclusion agreement terms and notification templates for currently excluded patrons.

5.7 The venue must have a procedure for responding to requests to access and correct personal information[7] collected about patrons for the purposes of FRT, in accordance with the *Privacy Act 1988*. Requests for access to information must be responded to within a reasonable period, which should not exceed 30 calendar days.[8] Where a request has been denied, the venue must provide written notice to the patron outlining the reasons for refusal and how to make a complaint. The Office of the Australian Information Commissioner provides guidance on dealing with requests for access to personal information.

6. System performance and integrity

The following is a list of requirements to ensure the FRT meets minimum standards of performance and to ensure the system can reliably and accurately identify excluded patrons.

6.1 The venue must ensure it receives the findings of key system performance tests (see **Attachment A** for specific testing criteria) from the FRT provider at the time of installation[9] and intermittently thereafter, confirming remediation of any negative findings. The venue must provide test reports and remediation evidence to Liquor & Gaming NSW on request.

6.2 The responsible person[10] at the venue must review FRT system usage reports at least weekly for larger venues[11] or monthly for smaller venues[12], noting information on the number of excluded patrons identified against the total number of faces scanned, time of identification, False Negative Identification Rates (FNIR)[13] and False Positive Identification Rates (FPIR)[14], and incidents of system disruption or downtime. The venue must also provide system reports to Liquor & Gaming NSW on request.

6.3 The responsible person at the venue must use the system logging function[15] to report on the time of contact with a matched patron and the accuracy of the notification, instances where FRT fails to identify an excluded patron if that patron is identified by staff, and suspected system errors. The venue must also ensure that FRT providers investigate and rectify any issues reported in the system log.

6.4 FRT must be operating during venue gaming machine trading hours. In case of any unplanned system outages or disruptions, the venue's internal control procedures must include measures to mitigate any reduced capacity to identify excluded patrons. For example, additional staff monitoring of the gaming area.

6.5 The venue must ensure that scheduled maintenance of FRT is planned and conducted outside of trading hours or, if not practical, during slow trading periods when fewer patrons are using gaming machines.

6.6 The venue must implement a complaint mechanism for patrons or the public to report concerns about the use of FRT in the venue. This need not be separate, or in addition, to any existing complaint mechanism that the venue already operates. The venue should forward technical complaints to the FRT provider for appropriate action and response. Liquor & Gaming NSW can provide advice on appropriate responses to other concerns, including privacy related matters.

[7] Personal information captured by FRT includes images captured by a FRT camera, biometric template data, FRT system metadata (this may vary between FRT systems but may include match confidence percentage and reason for match i.e. matched with exclusion database) and system metadata (including data, time and location of image capture, venue metadata (this may vary venue to venue but may include customer ID or customer status (i.e. customer loyalty tier))
[8] Venues that use FRT with existing ClubSafe and BetSafe exclusion registers should direct any patrons interested in reviewing and/or amending their personal information to the relevant exclusion register.
[9] Venues with existing FRT installed may retrospectively request performance test results and confirm remediation of any negative findings.
[10] The responsible person is the Responsible Gambling Officer (RGO), where applicable, or venue supervisor or manager, where not.
[11] A larger venue is defined as having 100+ or more EGMs connected to the Centralised Monitoring System.
[12] A smaller venue is defined as having less than 100 EGMs connected to the Centralised Monitoring System.
[13] FNIR is the percentage of excluded patrons who enter the venue or gaming area but are missed by the FRT system.
[14] FPIR is the percentage of non-excluded patrons who enter the venue or gaming area and are incorrectly matched by the FRT system.
[15] The system log should not be confused with the gambling incident register which focuses on events associated with gambling harm.

The venues must provide complainants with timely feedback on the outcome of any concerns raised.

7. Venue staff response to positive matches

The use of FRT in conjunction with exclusion registers is intended to assist a venue with its harm minimisation obligations by alerting staff to *potentially* excluded patrons. The technology is not intended to be a replacement for the identification and management of excluded patrons. It is intended to assist venues to meet their responsibilities regarding self-exclusion.

The following is a list of requirements to ensure venue staff can effectively manage a positive match by the FRT system.

7.1 The venue's internal control procedures must ensure that authorised staff receive notification of a positive match via the FRT user device within 60 seconds. Any incidence of a notification not occurring within 60 seconds of a match should be recorded in the gambling incident register.

7.2 Following an alert, the person responsible in the venue (an RGO, venue supervisor or manager) must approach the identified patron without delay.

7.3 The responsible person should not assume the system has accurately identified an excluded patron. They must first confirm the identity of the excluded patron before politely asking them to exit the gaming area or venue, while also considering the patron's dignity and privacy.

7.4 The responsible person must follow all relevant requirements under the Responsible Conduct of Gambling (RCG) training framework when interacting with the identified patron, including recording reportable incidents in the gambling incident register.

7.5 Following the interaction, the responsible person must log the time and outcome of the approach into the system log without delay.

Attachment A – Checklist of technical and operational requirements for FRT providers

The following is a checklist of technical and operational requirements for venues to provide to their primary FRT provider[1]. It is strongly recommended that FRT providers complete this checklist and sign the statutory declaration at the end of the document and return it to the venue.

FRT provider details

Please use the spaces below to fill out the details of your FRT company and product name, provide a brief description of the FRT technology, and list the name of the venue where the technology is being installed.

Company name: .....

Product name: .....

Product description: .....

.....

.....

.....

Venue name: .....

Privacy impact assessment (PIA) and data breach response plan

Requirement	Yes	No
The FRT provider organisation is treated as an "APP Entity" under the *Privacy Act 1988* (Privacy Act)	☐	☐
Any necessary support has been given to the venue to complete a Privacy Impact Assessement (PIA) on the FRT product, tailored to the specific venue setting.	☐	☐
A data breach response plan has been prepared for the FRT product, detailing procedures and clear lines of authority in the event of a suspected or confirmed data breach.	☐	☐

[1] The Code recognises that FRT encompasses several integrated components. The 'primary' FRT provider is the organisation that serves as the main point of contact for venues.

In the event of a data breach, the Australian Information Commissioner and individuals and organisations affected by the incident will be notified in line with the requirements under Part IIIC of the Privacy Act.	☐	☐

If 'No' to any of the above, please state the reason/s:

.....

.....

.....

.....

Installation and maintenance

Requirement	Yes	No
The hardware provider and installer hold a Class 2 security licence.	☐	☐
The venue's internet connection is adequate to ensure optimal operation and reliability of the FRT system.	☐	☐
Fixed Video Capturing Devices (FVCDs) are located within the licensed premises.	☐	☐
FVCDs are positioned to provide the best opportunity to capture the front facial profile of patrons entering the venue or gaming areas (depending on the venue, which may choose entry-based or gaming room-based cameras).	☐	☐
An adequate number of FVCDs have been installed to achieve full coverage of all possible entry points to the venue premises or gaming areas.	☐	☐
FVCDs are full HD resolution (1080p or better).	☐	☐
Consideration has been given to the optimal frame rate and shutter speed settings, and focal length specifications to enable clear, sharp images to be captured at the relevant subject-to-camera distance.	☐	☐
Environmental factors which may impact on image quality and accuracy of the FRT have been identified and mitigated using appropriate measures.	☐	☐
Guidance has been provided on the storage location of user devices and venue staff instructed on how to operate the devices.	☐	☐
The venue has been provided with detailed installation documents, including FRT hardware and software specifications, configurations, and settings.	☐	☐
The venue will be provided with updates on any significant hardware or software modifications that impact the functionality of the FRT.	☐	☐

If the venue has a hardware service agreement with the FRT provider, a technician is always on hand during the venue trading hours and can provide same-day response and complete repairs as soon as practical.	☐	☐

If 'No' to any of the above, please state the reason/s:

.....

.....

.....

.....

Data storage and transmission

Requirement	Yes	No
Data stores required to operate the system are located in Australian servers and subject to Australian data laws and governance.	☐	☐
The FRT can make multiple authenticated "Get" requests from the venue's data store, "Consume" excluded patron data and send "Push" notifications and/or SMS/email to a secure user device.	☐	☐
Data transmissions required to operate the system use end-to-end encryption, a firewall protected webserver (HTTPS), and a secure data exchange format (JSON).	☐	☐
Data is encrypted at a minimum 256-bit AES at rest and using Transport Layer Security (TLS) 1.3 or better in transit.	☐	☐
The FRT only accesses data necessary for the specific task of matching an excluded patron, including the patron's image and their name or a unique identifier.	☐	☐
The FRT does not video record or store images or metadata for patrons not excluded or matched against the exclusion register.	☐	☐
Biometric signatures and images of patrons are discarded immediately if not matched to an excluded person.	☐	☐
Any personal data of previously excluded patrons, including biometric signatures, is purged from the FRT system immediately following expiry or revocation of the self-exclusion.	☐	☐
Automatic deletion or workflow creation mechanisms are in place to ensure all data purging activities occur when required.	☐	☐
The FRT is set up to capture updates to the primary exclusion database at least daily.	☐	☐

The FRT incorporates data backup and disaster recovery measures for critical data, while ensuring compliance with the above data retention requirements.	☐	☐

If 'No' to any of the above, please state the reason/s:

.....

.....

.....

.....

Data access and use

Requirement	Yes	No
The FRT has access control mechanisms in place, including Multi-Factor Authentication (MFA), role-based permissions, and auto logout.	☐	☐
Edge servers that contain excluded patron information, including biometric signatures, are kept under lock and key and are capable of being erased remotely.	☐	☐
There are documented control processes for authorising staff access to the system, including procedures for onboarding staff with specific system roles, temporary privilege escalations, and immediate removal of users who exit their role.	☐	☐
The FRT incorporates an audit mechanism to monitor and log user access and events, including changes to user access rights, system configurations or excluded patron profile data.	☐	☐
The FRT will not be used in the venue for any commercial or marketing application.	☐	☐
The FRT is able to provide non-identifiable system data for performance evaluation and improvement or to support public health research or relevant policy development.	☐	☐

If 'No' to any of the above, please state the reason/s:

.....

.....

.....

.....

System performance and integrity

Requirement	Yes	No
The FRT is able to provide daily system usage reports to the venue, including total number of faces scanned, number of excluded patrons identified, time of the identification, False Negative Identification Rate (FNIR) and False Positive Identification Rate (FPIR), and incidents of disruption or downtime.	☐	☐
The FRT supports a manual logging function for authorised venue staff to record events that relate to the performance of the system, including time of contact with a matched patron, accuracy of the notification, instances where FRT fails to identify an excluded patron, and suspected system errors or biases.	☐	☐
There is a customer support function capable of providing effective and timely responses to critical and non-critical system failures and general system enquiries.	☐	☐
In the last 12 months, the FRT has demonstrated FNIRs and FPIRs and search speeds that are consistent with current National Institute of Standards and Technology (NIST) benchmarks2 across different demographic groups.	☐	☐
The FRT has a continuous health monitoring function, diagnostic tools, and updates software regularly to ensure reliable system performance.	☐	☐
The FRT includes intrusion and anomaly detection applications that monitor the system for suspicious activity and trigger an appropriate response.	☐	☐
The venue will be sent a quarterly report confirming that the FRT is operating correctly and complies with the technical requirements in this code, including key results of relevant functional tests and details of remediation measures, where applicable.	☐	☐
The FRT averages three nines of uptime (99.9%) or better during venue trading hours when it is expected to operate, incorporating redundancy components to limit instances of downtime.	☐	☐
Scheduled maintenance of FRT will be planned and conducted outside of trading hours or when gaming machines are not in use.	☐	☐
The venue will be notified at least 72 hours in advance of any planned maintenance activity which may result in disruption to the system.	☐	☐
A penetration test has been performed by a certified independent tester3 in the previous 12 months, including remediation of vulnerabilities, where applicable. Further penetration testing will be performed with any major feature enhancements or system configuration changes.	☐	☐

[2] Refer to the NIST Face Recognition Technology Evaluation (FRTE) and Face Analysis Technology Evaluation (FATE) test program. https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate

[3] Refer to the Digital NSW "Test and Verify Security" webpage for a list of recognised industry certifications.

If ‘No’ to any of the above, please state the reason/s:

……

……

……

……

Statutory Declaration

OATHS ACT 1900, NSW, NINTH SCHEDULE

I, ... , of ……..……
[name of declarant] *[residence]*

do hereby solemnly declare and affirm that:

the Checklist I have completed, titled "Attachment A – Checklist of technical and operational requirements for Facial Recognition Technology providers", is true and correct to the full extent of my knowledge.

And I make this solemn declaration, as to the matter (or matters) aforesaid, according to the law in this behalf made – and subject to the punishment by law provided for any wilfully false statement in any such declaration.

Declared at: ..... on .....
[place] *[date]*

.....
[signature of declarant]

in the presence of an authorised witness, who states:

I, ... , a .....,
[name of authorised witness] *[qualification of authorised witness]*

certify the following matters concerning the making of this statutory declaration by the person who made it: *[* please cross out any text that does not apply]*

1. *I saw the face of the person *OR* *I did not see the face of the person because the person was wearing a face covering, but I am satisfied that the person had a special justification for not removing the covering, and
2. *I have known the person for at least 12 months *OR* *I have confirmed the person's identity using an identification document and the document I relied on was ……...……..
[*describe identification document relied on]*

....
[signature of authorised witness] *[date]*

McKell Building
2-24 Rawson Place
Haymarket NSW 2000

GPO Box 7060
Sydney NSW 2001

Office hours:
Monday to Friday
9.00am — 4.00pm

T: 1300 024 720
E: contact.us@liquorandgaming.nsw.gov.au
W: www.liquorandgaming.nsw.gov.au

NSW GOVERNMENT