Digital Incident Register Guidelines

NSW GOVERNMENT

An incident register is a record of certain types of incidents that occur at a licensed venue.

This fact sheet sets out the key components of keeping and maintaining a digital incident register or digital gambling incident register.

Information on incident registers in general including requirements and benefits can be found here

A digital incident register (DIR) must include pre-designated fields for recording information on any reportable incident types.

Any DIR must include mandatory, voluntary and/or pre-filled fields with standardised text in line with the approved incident register book. Required fields include:

- date and time
- location of incident
- incident type
- capacity for recording additional details when reporting on mandatory incident types
- incident details, actions taken/summary outcomes
- witness details and
- persons of interest details.
- if police were notified or attended the incident

Additional fields outside of those required can also be created to fit the individual needs of a business.

All incident reports must be completed as soon as possible, and within 24 hours.

Required software security and data integrity features

Software for a DIR must provide the following features:

- ability to restrict access to approved staff members or users - via username/password or other means
- a system for managing an approved user list
- creating and deleting approved users
- ability to support multiple approved users
- automatic system log out after a set period of inactivity
- automatic assignment of an unalterable, sequenced unique identifier for each incident record
- automatic assignment of unalterable real-time dates and times for each register entry and updates
- mandatory date and time fields for incidents
- automatic assignment of an approved user name - via login - to each entry which includes incident reporting and updates
- no capacity to delete or edit existing incident records, but allows relevant information to be added at a later date
- an audit trail capacity that ensures all versions of any incident are saved and available for review upon request. For example an audit trail that ensures all versions are saved and can be viewed separately
- ability to flag incomplete entries for reportable incidents
- ability to flag entries for reportable incidents where details were not recorded within 24 hours.

Accessing information in the register and reporting

Any information recorded in the DIR, and any reports generated from it, must be able to be:

- made immediately available upon request by a police officer or inspector
- copied, printed or sent digitally so that it can be removed from the venue upon request by a police officer or inspector, and
- retained for a period for a least three years from when the record was made.

Licensed venues must be able to access any digital data records upon request regardless of any contractual arrangements with the software or internet provider.

Venues may choose to download their DIR reports as electronic documents or print out paper-based versions of incident reports.

The DIR software must also:

- support search and reporting functions for extracting incident records by date, time, date and time range, day of week, year, incident type, reportable incidents, flagged incidents, system user
- be able to be exported, upon request, in an appropriate digital form (excel or CSV) with each incident assigned to an individual row.

Which government bodies can view an incident register?

Liquor & Gaming NSW inspectors and police can review incident registers when they audit a licensed premises, take copies of any incident register, or remove any register from a licensed premises.

It is an offence to not produce the incident register upon request (as well as previous registers from the past 3 years).

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