



Nevada Gaming Control Board

Initial Cybersecurity Incident Response

A cybersecurity incident is any act in which a person has gained unauthorized access to an information system of a covered entity for purpose of disrupting, disabling, destroying, or controlling the system or destroying or gaining access to the information contained therein.

Pursuant to NGC Regulation 5.260(4)(b) A covered entity that experiences a cybersecurity incident relating to its information system that has resulted in a material loss of control, compromise, unauthorized disclosure of data or information, or any other similar occurrence shall:

Complete and submit an Initial Cybersecurity Incident Response report within 5 calendar days after activating the response procedures set forth in its cybersecurity incident response plan. Email this form to GCBCyber@gcb.nv.gov

REPORT BY

First Name:..... Last Name:
Position:
Phone: Mobile (Optional):
Email:

LICENSEE AND/OR SITE LOCATION(S) AFFECTED

Licensee Name:

Site(s)/Location(s) Affected:

Data Breached/Exfiltrated: Yes No

Systems affected: Server:

Network:

Other :

Gaming systems affected: Slot accounting/cashless wagering:

Kiosks:

If affected, identify the system Count room:

name and manufacturer. Player tracking/Patron management:

Table games:

Promotional/bonusing:

Race book and sports pool:

Inter-Casino linked systems:

Other:

INCIDENT DETAILS

Date/Time of Occurrence:

Date/Time Detected:

Type of Incident (Ransomware, Data Breach, Malware, etc.):

Incident Status: Resolved Unresolved Contained

Are you still open for business? Yes No Partial:

If closed, what time/date of closure occurred?

If closed, what time/date do you anticipate reopening?

Have you contacted another law enforcement agency? Yes No

Name of agency contacted (FBI, USSS, HSI, LVMPD, etc.):

INCIDENT SUMMARY

1. Provide a brief summary of the incident along with available technical details.
2. Identify the physical location of the systems affected.
3. If the attack resulted in a compromise or disruption to service, provide details of the impact.
4. Is the cyber security attack or data breach public information?
5. If information was accessed, have customers, clients, vendors, etc. been notified?
6. Identify the procedures in place to safeguard assets (funds in a cage, all gaming areas, drop boxes, count room).
7. Do you have adequate security personnel on the property to ensure compliance with standards/procedures?
8. What are the next steps you anticipate taking?
9. What third-party incident response firm has been hired to investigate/resolve the incident?

Add additional sheets as needed