



Nevada Gaming Control Board

Initial Cyber Incident Response

Pursuant to NGC Regulation 5.260(4) A covered entity that experiences a cyber attack to its information system resulting in a material loss of control, compromise, unauthorized disclosure of data or information, or any other similar occurrence shall: Provide written notification of the cyber attack to the Board as soon as practicable but no later than 72 hours after becoming aware of the cyber attack.

A cyber attack is any act or attempts to gain unauthorized access to an information system for purpose of disrupting, disabling, destroying, or controlling the system or destroying or gaining access to the information contained therein.

Email this completed 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: Servers
 Network
 Other:
Gaming systems affected: Slot accounting/cashless wagering:.....
 Kiosks:.....
If affected, identify the system name and manufacturer. Count room:.....
 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 the 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?

Add additional sheets as needed

