13:69D-1.11 Casino licensee's organization

(a) (No change.)

(b) In addition to satisfying the requirements of (a) above, each casino licensee's system of internal controls shall include, at a minimum, the following departments and supervisory positions. Each of the departments and supervisors required or authorized by this section (a "mandatory" department or supervisor) shall cooperate with, yet perform independently of, all other mandatory departments and supervisors of the casino licensee. Mandatory departments and supervisory positions are as follows:

1. (No change.)

2. An internal audit department, which may perform functions and fulfill responsibilities for multiple but affiliated casino licensees, supervised by a person, who shall be located in New Jersey, referred to in this section as an audit department executive. The audit department executive shall be subject to the reporting requirements specified in (c) below. The internal audit department shall be responsible for, without limitation, the following:

   i. The review and appraisal of the adequacy of internal control;

   ii. The compliance with internal control procedures;

   iii. The reporting to the Division of instances of noncompliance with the system of internal control;

   iv. The reporting to the Division of any material weaknesses in the system of internal control;

   v. The recommendation of procedures to eliminate any material weaknesses in the system of internal control[; and

vi. A quarterly review of information technology (IT) data security of the gaming systems if the casino offers Internet or mobile gaming];

3. An Information Security Officer (ISO) responsible for compliance with all IT security related regulations and statutes and licensed as a casino key employee. The ISO may be employed by the casino licensee or alternatively by a qualified holding or intermediary company of the casino licensee upon a showing to the Division that the responsibilities set forth herein can be satisfied. The ISO shall report directly to the audit committee of the board of directors, and shall:

i. Serve as the primary liaison to executive management and the Division for all matters regarding all aspects of information security;

ii. Have responsibility for all aspects of the licensee's investigation and response for IT security related incidents. The ISO shall immediately inform the Division, audit committee, and executive management on all incidents concerning:

a. Unauthorized access to or disclosure of critical data or confidential patron data;

b. Unauthorized system modification by a third party;

c. Unauthorized destruction of regulated IT assets or data; and

d. Any attack which compromises the availability or operation of any controlled computer system.

iii. Establish policies and procedures for monitoring employee access and ensuring deactivation of accounts assigned to terminated or suspended employees.

iv. Coordinate the development of a Business Continuity Plan with all of the licensee's business units, continually review the plan to ensure it remains current and compliant with National Institute of Standards and Technology (NIST) standards, and review the results of any test of the plan to ensure it is properly executed.

v. Approve the scope and review the results of any vulnerability scans and penetration tests. Review and approve resulting corrective action plans.

vi. Develop, document, audit, and enforce an information security plan consisting of policies, guidelines, standards, processes, and procedures in accordance with NIST standards. The ISO shall be responsible for continual evaluation of all areas of the plan described by this subsection in order to ensure the plan is responsive to new security threats, laws, or regulations. These areas include:

(1) Risk Management. The ISO shall create a risk management framework for all IT systems. In developing this framework, the ISO shall:

a. Utilize quantitative and qualitative based analysis to identify and rank all IT systems based upon risk;

b. Document the criteria used to determine risk for each system; and

c. Establish minimum security standards for all systems based upon risk.

(2) Personnel. The ISO shall be responsible for the:

a. Evaluation of the licensee's IT staffing levels and recommend any

changes needed to ensure protection of the IT infrastructure;

b. Creation of a standard for the proper segregation of IT job duties including appropriate levels of account privileges;

c. Evaluation of compliance with IT job segregation standards; and

d. Development of IT security training for employees.

(3) Systems and Data. The ISO shall ensure the information security plan addresses:

a. Protection of confidential patron data from unauthorized access;

b. Creation of required logs, with controls to prevent unauthorized modification; and

c. Existence of proper controls and documentation for changes and updates and patches to IT systems.

4. An IT department comprised of at a minimum an IT department manager[, IT security officer], and, if the licensee offers Internet and mobile gaming, an Internet and mobile games manager, all of whom shall be located in New Jersey and licensed as a casino key employee.

i. The IT department manager shall be responsible for the integrity of all data, as well as the quality, reliability, and accuracy of all computer systems and software used by the casino licensee **in accordance with the framework established by the Information Security Officer. This shall apply to** [in] the conduct of casino and casino simulcasting facility operations,

whether such data and software are located within or outside the casino hotel facility, including, without limitation, specification of appropriate computer software, hardware, and maintenance of:

(1) Access codes and other computer security controls used to insure appropriately limited access to computer software and data;
(2) Monitoring logs of user access, security incidents and unusual transactions;
(3) Logs used to document and maintain the details of any hardware and software modifications;
(4) Computer tapes, disks, or other electronic storage media containing data relevant to casino operations; and
(5) Computer hardware, communications equipment and software used in the conduct of casino operations;

[ii. The IT security officer shall report to the IT department manager and be responsible for:

(1) Maintaining access codes and other computer security controls used to insure appropriately limited access to computer software and data; and
(2) Reviewing logs of user access, security incidents, and unusual transactions;
(3) Coordinating the development of the licensee's information security policies, standards, and procedures;
(4) Coordinating the development of an education and training program on information security and privacy matters for employees and other authorized users;
(5) Ensuring compliance with all State and Federal information security policies and rules;
(6) Preparing and maintaining security-related reports and data;
(7) Working with internal and external audit personnel to ensure all findings

are addressed in a timely and effective manner;

(8) Developing and implementing an Incident Reporting and Response System to address security breaches, policy violations, and complaints from external parties;

(9) Serving as the official contact for information security and data privacy issues, including reporting to law enforcement;

(10) Developing and implementing an ongoing risk assessment program that targets information security and privacy matters by identifying methods for vulnerability detection and remediation and overseeing the testing of those methods; and

(11) Remaining current with the latest IT security and privacy legislation, rules, advisories, alerts, and vulnerabilities to ensure the licensee's security program and security software is effective; and]

iii. The Internet and/or mobile gaming manager shall report to the IT department manager, or other department manager as approved by the Division, and be responsible for ensuring the proper operation and integrity of Internet and/or mobile gaming and reviewing all reports of suspicious behavior;

4. - 6 (Renumber as 5. - 7.) (No change in text.)

(c) - (h) (No change.)