24 NCAC 06A .0407 INFORMATION SECURITY RESPONSIBILITIES

(a) The Internal Controls shall ensure that an Operator effectively implements its information security program in compliance with this Chapter and effectively allocates information security function responsibilities.

(b) The Operator shall implement, maintain, and comply with its comprehensive information security program as described in the Internal Controls, the purpose of which shall be to protect the confidentiality, integrity, and availability of Personal Information and other identifying information listed at G.S. 14-113.20(b) that is in its possession or in the possession of those entities acting on the Operator's behalf or under its direction.

(c) The Operator's information security program shall contain administrative, technical, and physical safeguards appropriate to the size, complexity, nature, and scope of the operations and the sensitivity of the Personal Information and other identifying information listed at G.S. 14-113.20(b) owned, licensed, maintained, handled, or otherwise in the possession of the Operator or in the possession of those entities acting on the Operator's behalf or under its direction.

(d) With respect to allocating security function responsibilities, the Operator shall utilize in its organizational structure an information security forum and an information security department as described in Paragraph (f) of this Rule.

(e) The Operator shall formally establish an information security forum or other organizational structures comprised of senior managers to monitor and review the information security program to ensure the program's suitability, adequacy, and effectiveness.

(1) The forum or other structures shall maintain formal minutes of meetings and convene at least every six months.

(2) The Operator's chief security officer or equivalent head of the information security department shall be a full member of the information security forum and be responsible for recommending information security policies and changes.

(f) The Operator shall maintain an information security department that is responsible for developing a security strategy in accordance with the overall Wagering operation. The information security department will subsequently work with the Operator's other departments, Affiliates, or Responsible Parties to implement and maintain the associated action plans. The department shall:

(1) be involved in reviewing tasks and processes that are required from the security perspective for the Operator, including, but not limited to, the protection of information and data, communications, physical, virtual, personnel, and overall business operational security;

(2) report to no lower than executive level management and shall be independent of the information technology department with regard to the management of security risk; and

(3) have the competences and be sufficiently empowered and have access to resources needed to enable the adequate assessment, management, and reduction of risk.

History Note: *Authority G.S. 18C-114(a)(14);*
Previously adopted as Rule 1D-007;
Eff. January 8, 2024;
Readopted Eff. March 27, 2024.