

1. Introduction

Olympus Holdings N.V., a Curacao registered company regulated by the Curacao Gaming Control Board (GCB) (the “Company”).

The Company is operating under the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen, P.B. 1993, no. 63) (NOOGH).

2. Policy

In line with the foregoing, it is the policy of the Company that information, as defined hereinafter, in all its forms -- written, spoken, recorded electronically or printed – will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All documentation, which may be in electronic form, must be retained for at least 7 (seven) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity and/or department within Company.

At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

3. Scope

The scope of information security includes the protection of the confidentiality, integrity and availability of information.

The framework for managing information security in this policy applies the Company entities and workers, and other Involved Persons and all Involved Systems throughout the Company, as defines below under the heading “Information Security Definitions”.

This policy and all standards apply to all protected personal information and other classes of protected information in any form as defined below under the heading 'Information Classification'.

4. Risk Management

A thorough analysis of all the Company's information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats- internal or external, natural or manmade, electronic and non-electronic – that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threat. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

Based on the periodic assessment, measures will be implemented that reduce the impact of the potential threats by reducing the amount and scope of the vulnerabilities.

5. Information Security Definitions

- a) **Affiliated Covered Entities:** Legally separate, but affiliated, entities, which are covered by this Information Security Policy.
- b) **Availability:** Data or information is accessible and usable upon demand by an authorized person.
- c) **Confidentiality:** Data or information is not made available or disclosed to unauthorized persons or processes.
- d) **Integrity:** Data or information has not been altered or destroyed in an unauthorized manner.
- e) **Involved Persons:** Every worker at the Company – no matter what their status. This includes employees, contractors, consultants, temporaries, volunteers, interns, etc.
- f) **Involved Systems:** All computer equipment and network systems that are within that Company environment. This includes all platforms (operating systems), all computer sizes

(personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

- g) Personal Information: Information related to a living who can be identified from such information or such information and other information in the possession of, or likely to come into the possession of, the Company (such information may include, but is not limited to, personal details such as name, address, date of birth, contact details, employment details, assets and liabilities, identification number, passports, driver's license etc...., as well as other financial information related to a living individual who can be identified from such information or from such information and other information in the possession of, or likely to come into the possession of, the Company;
- h) Proprietary Information: All information relating to the business, plans, intellectual property and/or technology of the Company including, but not limited to technical information including inventions, methods, plans, processes, specifications, characteristics, assays, raw data, scientific preclinical or clinical data, records, databases, formulations, clinical protocols, equipment design, know-how, experience, and trade secrets; developmental, marketing, sales, customer, supplier, consulting relationship information, operating, performance, and cost information; computer programming techniques whether in tangible or intangible form, and all record bearing media containing or disclosing the foregoing information and techniques including, written business plans, patents and patent applications, grant applications, notes and memoranda, whether in writing or presented, stored or maintained in or by electronic, magnetic, or other means, as well as all other materials containing information about the Company, as well as any other information specifically identified, either verbally or in writing, as proprietary to the Company;
- i) Protected Information: Comprises all information created or received by the Company, including, without limitation, the Company's Proprietary Information, as well as all Personal Information and/or Sensitive Information in the possession of, likely to come into the possession of the Company;
- j) Sensitive Information: Personal Information related to a living individual who can be identified from such information or from such information in the possession of, or likely to come into the possession of the Company, including, without limitation, information or data pertaining to:
 - i. race or ethnic origin
 - ii. religious beliefs or other beliefs of a similar nature,

- iii. political opinions,
- iv. physical or mental health or condition,
- v. sexual history or orientation,
- vi. trade union membership and/or
- vii. commission or alleged commission of any offense and any related court proceedings.

k) Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

6. Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information.

Regardless of classification the integrity and accuracy of all classifications of information must be protected

The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format.

The following levels are to be used when classifying information:

6.1. Protected Information

Protected Information comprises all information created or received by the Company, including, without limitation, the Company.

Unauthorized or improper disclosure, modification, or destruction of this information could violate applicable laws and regulations, result in civil and criminal penalties, and cause serious damage to the Company and its clients and/or their respective business interests.

6.2. Confidential Information

Confidential Information is very important and highly sensitive material that is not classified as Protected Information. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

Unauthorized disclosure of this information to people without a business need for access may violate applicable laws and regulations, or may cause significant problems for the Company, its clients, or its business partners. Decisions about the provision of access to this information must always be cleared through the Information Owner.