

Information Security Procedure

Softclub N.V.

Document Control

Version	Date	Description of Changes	Author
1.0	23.12.2025	Initial draft	IGA Trust B.V.

1. POLICY

It is the policy of SOFTCLUB N.V. 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 5 (five) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, with a period of time to be determined by each entity within SOFTCLUB N.V..

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.

2. SCOPE

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

The framework for managing information security in this policy applies to all SOFTCLUB N.V. entities and workers, and other Involved Persons and all Involved Systems throughout SOFTCLUB N.V. as defined below in INFORMATION SECURITY DEFINITIONS.

This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in INFORMATION CLASSIFICATION.

3. RISK MANAGEMENT

A thorough analysis of all SOFTCLUB N.V. 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 threats. 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 confidentiality, integrity, and availability of the information will be determined. The frequency of risk analysis will be determined at the entity level.

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

SOFTCLUB N.V. utilizes a number of protection mechanisms to prevent unauthorized access to the data and application software. Firewall controls are implemented to check for a number of common network attacks such as DOS, Synflood, Eavesdropping etc. DDoS attacks are handled with the help of ISP when support staff of SOFTCLUB N.V. issues a ticket with the datacenter asking for assistance in limiting the affect of such attacks. ISP should then start blocking ip addresses of attacking botnet. The stateful inspection of protocol enabled on the firewall also inspects protocols of higher level to help protect applications from hacking using known vulnerabilities in the code. To protect application code stored and executed on the servers checksums are compared to the referential database on a daily basis. The list of changed files (if any) is sent to system administrator for control and further actions. In order to prevent virus infiltration anti-virus software is scanning all files in system memory as well as those written to disks. Daily AV definitions updates followed by disks scans are invoked in the time of least system load.

4. INFORMATION SECURITY DEFINITIONS

Affiliated Covered Entities: Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity for purposes of HIPAA.

Availability: Data or information is accessible and usable upon demand by an authorized person.

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

Involved Persons: Every employee at SOFTCLUB N.V. - no matter what their status. This includes employees, contractors, consultants, temporaries, etc.

Involved Systems: All computer equipment and network systems that are operated within the SOFTCLUB N.V. 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.

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

5.. INFORMATION CLASSIFICATION

5.1 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:

5.2 Confidential Information

5.2.1 Confidential Information is very important and highly sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

5.2.2 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.

5.2.3 Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for SOFTCLUB N.V., its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

5.3 Internal Information

5.3.1 Internal Information is intended for unrestricted use within SOFTCLUB N.V., and in some cases within affiliated organizations such as SOFTCLUB N.V. business partners. This type of information is already widely distributed within SOFTCLUB N.V., or it could be so distributed within the organization without advance permission from the information owner.

5.3.2 Examples of Internal Information may include personnel directories, internal policies and procedures, most internal electronic mail messages.

5.3.3 Any information not explicitly classified as Confidential or Public will, by default, be classified as Internal Information.

5.3.4 Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

5.4 Public Information

5.4.1 Public Information has been specifically approved for public release by a designated authority within each entity of SOFTCLUB N.V.. Examples of Public Information may include marketing brochures and material posted to SOFTCLUB N.V. entity internet web pages.

5.4.2 This information may be disclosed outside of SOFTCLUB N.V..

6. COMPUTER AND INFORMATION CONTROL

6.1 All involved systems and information are assets of SOFTCLUB N.V. and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

6.2 Ownership of Software: All computer software developed by SOFTCLUB N.V. employees or contract personnel on behalf of SOFTCLUB N.V. or licensed for SOFTCLUB N.V. use is the property of SOFTCLUB N.V. and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

6.3 Installed Software: All software packages that reside on computers and networks within SOFTCLUB N.V. must comply with applicable licensing agreements and restrictions.

6.4 Virus Protection: Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

6.6 Data Transfer/Printing

6.6.1 Electronic Mass Data Transfers: Downloading and uploading Confidential, and Internal Information between systems must be strictly controlled. Requests for mass download of, or individual requests for, information for research purposes that include must be approved. All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Applicable Business Associate Agreements must be in place when transferring to external entities.

6.6.2 Other Electronic Data Transfers and Printing: Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise that is downloaded for educational purposes where possible should be de-identified before use.

6.7 Oral Communications: SOFTCLUB N.V. staff should be aware of their surroundings when discussing Confidential Information. This includes the use of cellular telephones in public areas. SOFTCLUB N.V. staff should not discuss Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

6.8 Audit Controls: Hardware, software, and/or procedural mechanisms that record and examine activity in information systems must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

6.9 Evaluation: SOFTCLUB N.V. requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic to ensure its continued protection.

6.10 Contingency Plan: Controls must ensure that SOFTCLUB N.V. can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain Confidential, or Internal Information. This will include developing policies and procedures to address the following:

6.11 Data Backup Plan:

- The Company shall maintain a documented and routinely reviewed Data Backup Plan designed to create, store, and maintain exact, retrievable copies of all critical digital records, including but not limited to:
 - Player identification and account data
 - Gaming activity and transaction logs
 - Financial transactions, payment records, and balances
 - AML, KYC, and compliance-related records
- Backups shall be performed at regular, predefined intervals in accordance with operational and regulatory requirements and retained for the period prescribed by the Curaçao Gaming Control Board (CGA) and applicable laws.

- All backup data shall be:
 - Stored in an off-site environment
 - Hosted on a Tier-IV certified data centre registered in Curaçao or an equivalent CGA-approved infrastructure
 - Protected against physical damage, environmental risks, unauthorised access, loss, or corruption

7. COMPLIANCE

7.1 The Information Security Policy applies to all users of SOFTCLUB N.V. information including: employees, and outside affiliates. Failure to comply with Information Security Policies and Standards by employees and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable SOFTCLUB N.V. procedures, or, in the case of outside affiliates, termination of the affiliation. Further, penalties associated with the legislation may apply.

Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorized disclosure of Confidential Information as specified in Confidentiality Statement.
- Unauthorized disclosure of sign-on code, username, id, or password.
- Attempting to obtain a sign-on code, username, id, or password that belongs to another person.
- Using or attempting to use another person's sign-on code, username, id or password.
- Unauthorized use of an authorized password to invade information for which there has been no request for review.
- Installing or using unlicensed software on SOFTCLUB N.V. computers.
- The intentional unauthorized destruction of SOFTCLUB N.V. information.
- Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

8. Password Control Standards

8.1 The SOFTCLUB N.V. Information Security Policy requires the use of strictly controlled passwords for accessing Confidential Information (CI) and Internal Information (II). Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

8.1.1 Standards for accessing CI, II: Users are responsible for complying with the following password standards

- Passwords must never be shared with another person, unless the person is a designated security manager.
- Every password must, where possible, be changed regularly – (between 45 and 90 days depending on the sensitivity of the information being accessed)
- Passwords must, where possible, have a minimum length of six characters.
- Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the ISO. This feature should be disabled in all applicable systems.
- Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.

8.1.2 When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc...). Combinations of alpha and numeric characters are more difficult to guess. Where possible, system software must enforce the following password standards:

- Passwords routed over a network must be encrypted.
- Passwords must be entered in a non-display field.
- System software must enforce the changing of passwords and the minimum length.
- System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15-minute timeframe. Lockout time must be set at a minimum of 30 minutes.
- System software must maintain a history of previous passwords and prevent their reuse.