INFORMATION SECURITY POLICY FOR NATIONAL BETTING AUTHORITY'S EXTERNAL USERS

VERSION HISTORY

Version Number	Date	Revised by	Reason for change
V1	21/04/2022	Compliance Officer	Translation of "010-01TG-Information Security Policy - Interested Parties-V3" Greek version
V2	29/03/2023	Compliance Officer	Translation of "010-01TG-Information Security Policy - Interested Parties-V5" Greek version

TABLE OF CONTENTS

SECTION 1 - INTRODUCTION

This Information Security Policy document consists of a set of rules enacted by the National Betting Authority's (the Authority) management to ensure that relevant external parties and networks within the organization meet the minimum requirements related to information security and data protection. Owner of this Policy is the Authority.

SECTION 2 - DEFINITIONS

IT: Information Technology

External Users: external business associates of the Authority and their personnel, government agencies, public authorities, prosecuting authorities and interested parties. The Authority's personnel and the members and President of its Board of Directors, internal and external consultants who use the premises and equipment of the Authority, are governed by the Information Security Policy of the organization, which is specified in a separate, more extensive document.

SECTION 3 – KEY PRINCIPLES

3.1 Information Technology Systems (IT Systems) are to be protected from unauthorized access at all times.

3.2 IT Systems are to be used only in compliance with the relevant Policies and Procedures of the Authority.

3.3 The Authority shall ensure that the External Users have acknowledged (in writing or electronically) that they have read and understood the Information Security Policy for National Betting Authority's External Users as well as all other relevant Policies.

3.4 Data stored on IT Systems shall be managed securely in compliance with all applicable data protection legislation (including the EU's General Data Protection Regulation ("GDPR")).

3.5 Access to information and/or information systems shall be granted on a "need to know" and "least privilege" basis, as per an External User's job responsibilities.

3.6 Relevant technical and/or organizational controls shall be implemented to ensure that all data, both in physical and digital format, is protected against leakage and/or corruption.

3.7 All breaches of security pertaining to the IT Systems or any data stored thereon shall be officially reported from the External Users to the Authority and subsequently investigated by the Authority's IT Department as detailed in the internal procedures. Any breach which is either known or suspected to involve personal data shall also be reported to the Authority's Data Protection Officer.

3.8 External Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the Authority's IT Department. If any such concerns

relate in any way to personal data, such concerns must also be reported to the Authority's Data Protection officer.

3.9 Devices provided to External Users by the Authority should only be used for the sole purpose of conducting business related to the Authority.

SECTION 4 – ROLES AND RESPONSIBILITIES

4.1 External Users

External Users shall be responsible for ensuring that:

a. they are aware of the information security policies, the procedures and the user obligations that apply to their area of work,
b. they are aware of their personal responsibilities for information security,
c. they have appropriate training for the systems they are using,
d. they know how to access advice on information security matters,
e. their IT Systems which are used by third parties and include the Authority's information, have been assessed as suitable and are complying to the Authority's security requirements,
f. they are kept aware of the requirements of this Policy and of the related legislation and regulations,
g. a report is made to the Authority, where required, concerning security issues or failures arising from or coinciding with, their responsibilities,
h. they comply with all relevant parts of this Policy at all times when using the IT Systems,
i. under no circumstances should they make use of physical media (e.g., USB memory sticks or disks of any kind) for the transfer of files to the Authority's IT systems,
j. the use of the Authority's IT resources is conducted in a responsible manner and under no circumstances intentionally engaging in any of the following activities:
    - damaging or attempting to damage an information system,
    - attempting to access an information resource for which they have no access rights,
    - introducing or attempting to introduce any malicious code into an information system (e.g. a virus, a Trojan or other malware, etc.),
    - violating or attempting to violate the terms of use or license agreement of any software product used by the Authority.

4.2 Information security in project management

a. Information security shall be integrated into National Betting Authority's procedures to ensure that information security risks are identified and addressed. The project management methods in use shall require that:
    - The information security objective is included in project objectives,
    - An information security risk assessment is conducted at an early stage of the project to identify necessary controls, and

- Information security is part of all stages of the applied project methodology.

b. Information security issues shall be addressed and reviewed regularly in all projects.
c. All the projects within National Betting Authority's scope shall undergo periodic security assessments.

SECTION 5 – PREMISES SECURITY POLICY

5.1 Access is authorized and based on an individual's job function. To that end, External Users must at all times use the personal access card provided to them by the Authority. Under no circumstances should an External User lend their access card to any other individual. Impersonation is illegal and strictly forbidden.

5.2 Access token (such as keys, access cards etc.) shall be returned immediately upon termination of an External User's contract or employment.

5.3 If an access token, such as a key or access card, is lost, shall be immediately reported to the Authority.

5.4 Visitors shall be identified and authorized before entering the Authority's premises and always be escorted and/or carry a visitor card.

SECTION 6 – ANTIVIRUS SECURITY MEASURES

6.1 IT Systems commonly affected by a virus (including all computers and servers) shall be protected with suitable anti-virus, firewall, and other internet security software. All such software shall be kept up to date with the latest software updates and definitions.

6.2 All IT Systems protected by anti-virus software shall be subject to a full system scan at least once per week. The virus definitions library shall be updated daily.

SECTION 7 – MOBILE DEVICES POLICY

7.1 Mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Authority should always be transported securely and handled with care. External Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or the Authority premises. If any such mobile device is to be left in a vehicle it must be stored out of sight and, where possible, in a locked compartment.

7.2 Mobile devices (including, but not limited to, laptops, tablets, and smartphones) shall be protected with additional security layers, such as a secure password or passcode or any other form of secure log-in system.

7.3 Mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Authority shall be set to lock, sleep, or similar, after a period of inactivity defined and set by the Authority, requiring a password, passcode, or other form of log-in to unlock, wake, or similar. External Users may not alter this time period.

SECTION 8 – PASSWORD POLICY

8.1 Passwords must, where the software, computer, or device allows:

a. be at least eight (8) characters long,
b. contain a combination of upper- and lower-case letters, numbers, and symbols,
c. be changed at least every three (3) months,
d. be different from the previous twelve passwords of the External User in question,
e. not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.).

8.2 Passwords shall be treated as sensitive and confidential information. In this respect, External Users shall not share their passwords with anybody within or outside the Authority including supervisors, managers, directors, family members, etc.

8.3 Passwords should under no circumstances be communicated over email, chat applications, or similar.

8.4 Where passwords need to be stored, they should always be stored securely using suitable software. Passwords should under no circumstances be written down or left on display.

8.5 If an External User forgets their password, this should be reported to the Authority to take the necessary steps to restore the External User's access to the Authority's IT Systems.

8.6 Passwords used for corporate access shall not be used for any other purposes such as accessing personal email accounts, personal banking, etc.

8.7 In case there is an indication that, the security/confidentiality of a password or other similar data that are used for confirming the user's identity, the user must change the password and/or similar data. In such a case, the change may be made unilaterally by the IT Department.

SECTION 9 – REMOTE ACCESS SECURITY POLICY

9.1 Remote access to the Authority's internal networks may be permitted to External Users under the following strict requirements:

a. External Users shall be given authorization from the Authority to remotely access the Authority's systems,
b. the access should be secured with a suitable encryption protocol (such as a Virtual Private Network) and strong passphrases. Passwords should adhere to the requirements set in the Password Policy (Section 8),

c. a remote connection should only be established through a host, equipped with the most up-to-date version of the anti-virus software as well as the most recent version (including any security patches) of all its applications and operating system,
authorized External Users should only instantiate a remote session while connected to their personal home network or the network of a trusted third-party. Connection through unsecured public networks (including cafes, restaurants, airports etc.) should be avoided.

9.2 The Authority reserves the right to unilaterally suspend or cancel an External User's telecommuting privileges at any time.

SECTION 10 – DATA CLASSIFICATION POLICY

10.1 Data within the Authority shall be classified to one of the classifications defined below:

- Strictly Confidential

Definition: Data in any format collected, held, and processed by or on behalf of the Authority that is subject to specific protections under national or European laws or regulations or applicable contracts.

Examples: Records containing personal data of individuals, such as employee records, records of the personnel of regulated legal persons, records of regulated physical persons, contracts with external third parties, betting activity of individuals etc.

- Confidential

Definition: Data the loss, modification, or unauthorized disclosure of which could result to impairing the functions of the Authority, cause significant financial or reputational loss or lead to potential legal liability.

Examples: Internal reports, NBA Policies and Procedures, NBA telephone directory etc.

- For Internal Use Only

Definition: Data the unauthorized disclosure, modification, or destruction of which is not expected to impact the Authority seriously or adversely, its employees, any external contractors, or regulated entities.

Examples: Training material, Manuals, etc.

- License

Exclusively defined as the licenses for the provision of betting services which are issued by the Authority.

Examples: Class A bookmaker's licence, Class B bookmaker's licence, authorised agent's licence, premises' licence and person in charge of premises letters.

- Public

Definition: Data that does not fall into any of the other three categories and can be made publicly available without specific permission.

Examples: Public announcements, List of licensed entities (bookmakers, authorised agents, premises), Blocking List, Strategic Planning etc.

SECTION 11 – DATA PROTECTION POLICY

Confidential Data

11.1 In cases where confidential data needs to be transferred on electronic media or devices, and unless its confidentiality can be otherwise assured, it must be encrypted.

11.2 Confidential data to be transferred physically shall be transferred in a suitable container marked "Confidential" by a secure courier service or other approved delivery method that can be accurately tracked.

Confidential or Strictly Confidential Data

11.3 Confidential or strictly confidential data stored electronically on the Authority's IT Systems should be stored securely using controlled access.

11.4 Any printed records carrying confidential or strictly confidential data as defined in the Data Classification Policy (Section 10) are stored in locked compartments in access-controlled locations in the Authority's premises.

11.5 In cases where confidential or strictly confidential data needs to be transferred over networks, its confidentiality must be protected by means of appropriate encryption techniques.

11.6 Any printing or copying of confidential or strictly confidential data records should be avoided where possible and is only permitted using the Authority's printers and copiers, which are part of the internal network and thus protected by suitable network equipment (firewall).

Strictly Confidential Data

11.7 No strictly confidential data should be stored or transferred to any mobile device (including, but not limited to, laptops, tablets, and smartphones) or any transferable physical medium (including but not limited to USB memory sticks, or disks of any kind), whether such a device or medium belongs to the Authority or otherwise.

11.8 The physical transfer of printed records containing strictly confidential data shall be avoided whenever possible. In cases where physical transfer is necessary, these records shall only be transferred in a suitable container marked "Strictly Confidential" under the supervision of an authorized Officer of the Authority.

11.9 External Users handling strictly confidential data for or on behalf of the Authority shall be subject to, and must comply with the following provisions:

a. emails containing strictly confidential data must be encrypted and marked "strictly confidential",
b. strictly confidential data may be transmitted over secure networks only, transmission over unsecured networks is not permitted under any circumstances,

strictly confidential data contained in the body of an email, whether sent or received, should be stored securely.**11.10** Personal data (as defined in the GDPR) collected, held, and processed by the Authority will be strictly managed in accordance with the principles and provisions of the GDPR.

11.11 The Authority shall ensure that any personal data collected is only retained for as long as necessary to fulfill the purpose of its collection.

11.12 In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, the Data Protection Officer of the Authority shall be immediately notified to promptly assess the risk to people's rights and freedoms and, if appropriate, report this breach to the relevant Data Protection Authority.

Information transfer

11.13 Agreements, such as formal contracts and software escrow agreements, are established for the transfer or exchange of information and software between organizations and are compliant with the relevant legislation. Procedures are in place within each business area where information is received or transmitted to ensure that information transfers or exchanges are carried out securely and in accordance with National Betting Authority's policy requirements where applicable.

SECTION 12 – REPORTING SECURITY BREACHES

12.1 Concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Authority via telephone on 22881800 or submission of a relevant report through the Authority's website https://nba.gov.cy/en/incident-reporting-form/. Reports of security incidents shall be escalated to the appropriate members of the Authority's management without delay.

12.2 Concerns, questions, suspected breaches, or known breaches that involve personal data shall be referred immediately to the Authority and its Data Protection Officer to the email address dpo@nba.gov.cy or the telephone 22881800, who shall handle the matter in accordance with the Authority's Data Protection Policy.

12.3 Upon receiving a question or notification of a breach, the Authority's IT Department shall, within a reasonable timeframe, assess the issue including, but not limited to, the level of risk associated therewith, and shall take all such steps as the IT Department deems necessary to respond to the issue. If criminal action is suspected, law enforcement authorities must be contacted.

12.4 Under no circumstances should an External User attempt to resolve a security breach on their own without first consulting the Authority.

SECTION 13 – POLICY FOR THE INTERNET USAGE ON THE AUTHORITY'S PREMISES

13.1 External Users should use the Authority's Internet facilities responsibly and professionally at all times, in accordance with the execution of the required work.

13.2 The Authority provides Internet access to its External Users for the sole purpose of business and to assist them in performing their work.

13.3 Transferring large data volumes over the Internet shall be avoided during the usage of the Authority's Internet facilities.

13.4 External Users must under no circumstances use the Internet to gain or attempt to gain unauthorized access to Authority data or restricted areas of the Authority's network.

13.5 External Users must not attempt to download, view, or otherwise retrieve illegal, pornographic, sexist, racist, offensive or any other immoral material. The access to content that may offend any person or constitute a source of embarrassment to the Authority or otherwise tarnish its image and reputation is strictly prohibited.

13.6 The Authority's network equipment do not allow certain endpoints to access a number of websites. If an External User has genuine and specific business need to connect to such a blocked site, they must seek the approval of the Authority.

13.7 External Users need to be mindful of the different classification levels of data as those are defined by the Authority and consequently make sure that no confidential or strictly confidential data is ever disseminated in the course of communications over email.

SECTION 14 – SUPPLIER/VENDOR SECURITY POLICY

14.1 Contracted Suppliers and Vendors shall acknowledge that they have read and understood this Policy and all other Policies that are relevant to the service they provide.

14.2 External Users shall acknowledge that they have read and understood this Policy and all other Policies that are relevant to the service they provide.

SECTION 15 – ACCEPTABLE USE OF ASSETS

a. External Users shall be authorized to utilize National Betting Authority's information resources only for business purposes under which they execute their work and for which they have been authorized,
b. External Users shall terminate active sessions with the Authority when finished,
c. External Users are prohibited from changing the configuration, removing, de-activating, tampering with or bypassing any security controls such as antivirus or malware prevention/ detection software, modifying registry entries, logs on the Authority's devices and/or equipment used by them,

d. The installation or removal of software on or from the Authority's equipment shall only be implementable by authorized members of the Authority's IT Department.
e. External Users shall exercise caution when downloading files from the Internet and shall download only from legitimate and reputable senders/sources. They shall verify first that an anti-virus program has checked the files,
f. When in doubt, suspicious files or e-mail attachments shall not be opened, downloaded, or executed.

SECTION 16 – OPERATIONAL PROCEDURES AND RESPONSIBILITIES

16.1 Outsourced development

a. The requirements regarding development set out in this policy apply equally to any third-party products that are either purchased "off the shelf" or developed specifically for NBA. In addition, the following apply:
    - Contracts with third parties must address not only the business and end user requirements, but the security requirements also. Software facilitating excessive functionality at the expense of security controls are rejected,
    - Systems developed for the Organization by third parties are subject to thorough testing to ensure the quality and accuracy of the work carried out, as well as to detect any malicious code before the systems Go-Live.
b. Outsourced software development is supervised and monitored by the Authority's IT Department. Where software development is outsourced, the following are considered:
    - licensing arrangements, intellectual property rights and code ownership,
    - inquiring of the quality and system development procedures,
    - rights of access for audit of the quality and accuracy of work done.

SECTION 17 – POLICY REVIEW

The Policy is reviewed at least annually and updated as needed to reflect changes to business objectives and/or the risk environment. Updated versions of the Policy shall be immediately communicated to all External Users and other involved parties. Any questions, concerns, and other feedback relating to this Policy should be communicated to the Compliance Officer, complianceofficer@nba.gov.cy, and/or the Data Protection Officer, dpo@nba.gov.cy.

SECTION 18 – POLICY IMPLEMENTATION

This Policy shall be deemed effective as of March of 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date. Any and all deliberate or negligent breaches of this Policy by External Users will be handled as appropriate by the Authority.