



Netball Hong Kong, China

Information Security Policy

1. Core Obligations & Importance

As a National Sports Association (NSA) trusted by athletes and global sports bodies, Netball Hong Kong, China (NHKC) enforces rigorous mechanisms to secure data systems from unauthorized access, loss, or misuse.

- **Paramount Importance:** Information security is fundamental to our sporting integrity, NHKC mandates top-tier precautions to ensure data is always safe, secure, and confidential.
- **Protected Data Scope:** This policy safeguards all sensitive personal information of all netball-affiliated personnel—including athletes, coaches, team officials, umpires, office staff, committee members, and volunteers. Protected data includes, but is not limited to, passport and identity details, medical and anti-doping records, travel itineraries, banking and reimbursement data, contact details, and performance/evaluation statistics.
- **Threat Mitigation:** Comprehensive defenses are established to shield personal data from cyber-attacks, phishing, unauthorized disclosures, and accidental data leaks during cross-border sports administration.

2. Mandatory Security Measures

To guarantee a fully protected communication network and data environment, NHKC implements the following protocols:

- **Access Control:** Strict "need-to-know" access controls are enforced. Only authorized NHKC personnel are granted permission to handle sensitive personal data.
- **Password:** All authorized users must adhere to the mandatory use of complex passwords (incorporating a minimum length, upper/lowercase letters, numbers, and special characters) for all official accounts, systems, and devices, with regular required credential updates.
- **Contingency Planning:** A rapid-response data breach contingency plan is active. In the event of a suspected security incident, immediate containment actions will be deployed, and affected personnel will be notified within 48 hours.

3. Physical & Device Safeguards

All personnel issued or utilizing hardware containing NHKC or personal data must adhere to strict physical security standards:

- **Physical Device Protection:** Laptops, tablets, mobile phones, USB drives, and hard-copy files must never be left unattended in public spaces, shared transit, or unsecured venues.
- **Access Safeguards:** All devices accessing NHKC network systems must be protected by strong passwords or biometric locks, automatic screen lock timers (5 minutes maximum), and full-disk



encryption where applicable.

- **Storage Protocols:** Removable storage devices (e.g., flash drives) containing sensitive personal or organizational data must be encrypted and physically locked when not in active use.

4. Reporting Process for Lost or Stolen Devices & Data Incidents

To contain potential security breaches rapidly, any loss, theft, or compromise of a device must follow a mandatory reporting procedure:

- **Immediate Reporting Window:** If a device containing NHKC system access, personal data, or confidential files is lost, stolen, or compromised, the owner must report the incident to NHKC at nhkc@netball.org.hk within **2 hours** of discovery.
- **Mandatory Information Required:** The initial report must include:
 - Description of the device (type, model, and serial number).
 - Date, time, and location/circumstances of the loss or theft.
 - Scope of data stored on or accessible through the device (e.g., athlete records, emails, financial details).
 - Actions taken so far (e.g., local police report filed, remote lock initiated).
- **Containment & Remediation:** Upon notification, the Executive Committee will immediately revoke network access credentials, perform remote device wipes where applicable, and initiate the data breach contingency plan.

5. Account Management & Operating Protocols

- **Authorized System Operation:** Only designated office staff and specifically appointed personnel are authorized to operate, access, or manage official NHKC databases, administrative portals, and digital communication platforms. Unaccredited individuals or external parties are strictly prohibited from accessing, altering, or broadcasting through official NHKC data systems.
- **Prior Authorization for Data Disclosure:** All external disclosures of system data, statistical reports, or public data releases must be **pre-approved by NHKC**. Personnel are strictly prohibited from sharing, exporting, or making public statements regarding internal data assets without prior authorization from the Executive Committee or designated media and IT officers.

6. Operational Integrity & Safeguards

All authorized operators of NHKC systems and data assets must adhere strictly to the following operational standards across all public and internal data handling processes:

6.1 Strict Prohibitions on Unlawful & Sensitive Data Handling

Accessing, storing, or transmitting content containing the following via NHKC systems is strictly prohibited:

- **Political Content:** Political statements, partisan commentary, or campaign material.
- **Religious Content:** Proselytizing, religious debates, or posts promoting religious division.
- **Racial Content:** Racially insensitive remarks, slurs, hate speech, or racially charged

rhetoric.

- **Sexual Content:** Sexually explicit imagery, vulgar language, suggestive material, or inappropriate sexual commentary.
- **Harassment & Defamation:** Content involving cyberbullying, stalking, or defamatory statements that target or compromise athletes, umpires, officials, or sports partners.

6.2 Protecting Team Competitive Intelligence & Strategy

Personnel handling technical or tactical data systems must refrain from exposing sensitive internal information that could provide strategic intelligence to current or future opponents:

- **Tactical & Technical Data:** Detailed digital breakdowns of set plays, planned formations, set-play routines, or preparation strategies.
- **Strategic Adjustments & Vulnerabilities:** Digital records or communication threads covering preferred tactical adjustments, opponent-specific preparation, or strategic areas identified by coaching staff for targeted improvement.
- **Internal Communications & Confidentiality:** Digital records of internal team briefings, closed training logs, or private communications between coaching and support staff.
- **Athlete Privacy & Physical Status:** Non-public tournament lineups, injury reports, medical updates, or physical limitation metrics. Private or overheard details regarding an athlete's health, injury recovery, or fitness status must **not** be stored in unsecured channels or disclosed unless officially released by team management.

7. Commercial Endorsements & Institutional Values

- **Commercial & Data Rights:** Personnel must ensure that digital data assets, player imagery, and performance records are not used to endorse commercial products or personal sponsors without proper authorization. Personal commercial activities must not conflict with official NHKC commercial partners, event regulations, or local governing laws.
- **Brand Awareness:** Operational handling of data directly reflects on the association. Continuous care must be exercised across all digital platforms to uphold core organizational values and avoid legal liabilities.

8. Consequences of Non-Compliance

- **Strict Penalty Notice:** Any breach of this policy by staff, coaches, athletes, or affiliated personnel—including failure to report a lost or stolen device in a timely manner—will result in immediate disciplinary action, legal liability under Hong Kong law, and reporting to relevant statutory authorities. NHKC treats data protection as a serious breach of sports ethics and institutional trust.
- **Consequences of Breach:** Violations of this policy will lead to immediate review by the Executive Committee or designated disciplinary panel. Non-compliance may result in formal reprimands, immediate revocation of system access, removal from administrative or coaching duties, suspension from national selection, or loss of athlete representation privileges.