Nfield security whitepaper

Last updated: 23 July 2025

nipo

Contents

1. Introduction

Keeping your valuable data safe is an absolute priority for us. It's an obligation that guides everything we do when shaping and powering Nfield's features. Every conceivable measure is taken to ensure both our team and our software solutions comply with the highest security standards.

This whitepaper explores the essential components of a robust data security strategy, offering insights into best practices, and technologies designed to safeguard sensitive information. From encryption and access controls to data governance frameworks and incident response protocols, this paper provides a comprehensive overview of the tools and approaches required to mitigate risk in today's complex digital environment.

This whitepaper aims to equip professionals and decision-makers with the knowledge and strategies needed to protect their most valuable digital assets in an increasingly interconnected world.

Nfield security is underpinned by two core foundations

NIPO security

We maintain a strong security policy that ensures both your data, and our products are safeguarded round the clock. Independent security experts (ethical hackers) scrutinize our security procedures every year to evaluate our tools, processes and people. The measures to conform with ISO 27001:2022 for our Information Security Management System, as certified by an auditor (Auditor), are strictly followed in every wire connection and by every person in our company. As a matter of principle, the smallest possible number of NIPO specialists have access to Nfield's infrastructure for carrying out deployments and maintenance.

Microsoft security

Nfield runs on Microsoft Azure, the highly secured cloud known for its flawless, trusted performance, extensive data storage and reliability. Microsoft's engineers work 24/7 to protect the cloud, scale its powers and administer other services which run on it, including Office365. For more information, please visit the Microsoft Trust Center for up-to-date details on policies, processes, and practices that help you manage data control and comply with industry and government regulations.

2. Data handling & access control

Protecting the confidentiality, integrity, and availability of data
Ensuring compliance with legal, regulatory, and industry standards
Minimizing risks associated with data loss, breaches, or misuse

NIPO shall always maintain appropriate technical and organizational measures designed to protect the security, confidentiality and integrity of customer data.

We regularly monitor compliance with these measures. We are ISO 27001:2022 certified. On request, we can share the part of our annual ISO audit report relevant for assessing our compliance with data protection laws.

Nfield provides features that enable you to secure your domain to the highest level.

Strong authentication

Two-factor authentication (2FA): Nfield accounts secured with two-factor authentication require users to enter a code (a token) generated by a standard authenticator app on a mobile phone. This has the effect of complementing something you know (your username and password) with a code obtained through something you have (your phone). It effectively blocks any unauthorized access to your Nfield account, even from those who have obtained your username and password, as these people (or their machines) are unable to retrieve the second factor code from the phone. Your valuable Nfield fieldwork and respondent data is thereby protected from prying eyes. Learn more in our article Protecting your Nfield login with two-factor authentication.

Single-sign-on (SSO): For enterprises, Nfield can be set up to use Office 365 accounts for Nfield login. Administration of your Nfield user accounts, for as many Nfield domains as you have, is centralized in your organization's single-sign-on layer. In the case of an employee leaving the organization or other reason for revoking a person's system access (e.g. because of a security breach), Nfield will automatically be included in the revoked permissions, with immediate effect from when the account in the single-sign-on layer is disabled or reset. With SSO, your password policy for accessing Nfield is automatically aligned with that of your organization.

Strong password policy: Nfield can easily be configured to comply with strong password policies. Domain administrators can set rules for things such as password expiration period, old password re-use and strong password requirements (e.g. minimum number of characters and different character sets). You should also regularly revalidate your authorized users and ensure immediate removal of departing employees.

Private, individual domains

Your projects are stored in your own individual domain, inaccessible to anyone else – even our employees – unless explicitly requested by you for customer support purposes.

Any data created using Nfield is only stored in Nfield. It is not stored outside the Nfield system by NIPO or Microsoft. Information about your Nfield account and your Nfield usage is only available to users in your organization who have an Nfield domain administrator role. These domain administrators control what personal information is stored about you in Nfield. Nfield allows storing your username, your real name, your email address and your telephone.

Access control and logging

Nfield allows administrators to configure access on a user-by-user basis, defining the scope of activities every user is allowed to perform. Password requirements can also be set to enforce your chosen password policy, however strong you need it to be. All user actions are tracked and domain administrators can review them individually. The system automatically signs users out when inactive for more than 15 minutes.

Survey group access restriction

Surveys contain valuable, and sometimes sensitive, information. It's therefore essential to restrict access to certain parts of surveys to those who really need it to do their jobs. This is done by assigning users with specific roles which only allow access to designated areas and functionality. Find out more in our article Controlling access to survey rights. Setting the right access also limits the scope of risk in the case of data breach.

Data encryption and storage

Encryption standards (at-rest and in-transit)
Data storage policies (e.g., local, cloud, backup)
Encryption key management

Data encryption

All your data is secured by SSL and encrypted, both at rest and during transfer, to protect it from sniffing.

Encoded questionnaires

Nfield questionnaires are stored in an encoded proprietary format. The original script is never displayed in an interviewer's device, so interviewers cannot make changes.

Nfield's regional setup

Nfield is a cloud solution, currently offered from 4 Microsoft Azure centers. Each Nfield deployment has full geo replication in place:

Region	Primary location	Geo replication location	Primary location (for reporting)	Geo replication location (for reporting)
Europe and Africa	Amsterdam	Dublin	Amsterdam	Dublin
APAC	Hong Kong	Singapore	Singapore	Hong Kong
Americas	Virginia	California	Virginia	California
China	Beijing	Shanghai	N/A	N/A

3.

Local data storage option

Different countries and industries often have their own specific regulations when it comes to data storage. To comply with this, market research companies need to consider where their respondent data is stored. To enable data storage compliance, we have developed the ability to separate survey deployment from storage of respondent data. This means it is now possible, for example, to deploy a survey from the Hong Kong SAR Microsoft Data Center and store the respondent data in the Singapore Microsoft Data Center.

4. Data backup and disaster recovery

Backup frequency and data retention policies
Data recovery procedures (in case of data loss or system failures)
Testing of backup processes

Data backup

Your collected data is stored in secure Microsoft SQL database servers and replicated in other data centers so it can be restored in the event of something going wrong. Microsoft security policies strictly regulate access to its data centers.

Nfield disaster recovery

NIPO has Business Continuity Plans which are reviewed and tested regularly and include data backup recovery as well as applicable internal and external communication protocols. The plan also includes a listing of asset requirements and priorities for restoring applications within our remit.

- All data is replicated locally at least 3 times to prevent from hardware failure.
- All data is replicated geographically to prevent from data center failure, except for those domains that have the local storage feature and there's no secondary region.
- All data has minimum 30-day back-up to recover from software failure of malicious attempt.
- A disaster recovery test is carried out annually to test all the recovery scenario's that are available for Nfield.

The customer is responsible for deleting information from NIPO platforms. When a customer deletes any artifact, it is guaranteed to be deleted from the primary systems within 15 minutes (including geo-replicated systems) and from all back-ups within 30 days.

5. Data transmission and network security

Secure communication channels (e.g., VPN, TLS/SSL)
Network security protocols (firewalls, intrusion detection/prevention systems)
Protection of data in transit

Application security

All data in Nfield is segregated and encrypted both at rest and during transfer. Least privilege and deny all access policies are also in place at NIPO which is the same for access to key users.

All communication is securely encrypted using SSL, with the more secure, updated TLS 1.2 protocol, employing a SHA-256 cipher for encryption.

- Passwords are stored using salted hash and SHA-512 cipher.
- Data is stored using EAS 256 symmetric key for encryption (database and storage accounts).

NIPO is responsible for overarching system security (data of all customers).

Customers are responsible for securing access to their own tenant applications. NIPO offers tools to setup and maintain security and access policies to do so.

6. Incident management and response

Procedures for identifying and reporting incidents
Steps to respond to data breaches
Notification and communication protocols (internal and external)

Incident management

In the unlikely event of a security incident, NIPO has established a dedicated incident response team that implements a comprehensive plan to mitigate the impact effectively. This plan consists of the following key steps:

- Investigation: We promptly initiate an investigation to ascertain the cause and scope of the breach.
- Containment: Upon identifying the breach's source, we take immediate action to contain it and prevent any further unauthorized access to our systems.
- Notification: Affected customers are notified as soon as possible in accordance with legal and contractual obligations. We prioritize transparency and commit to keeping our customers informed about any potential security incidents.
- Remediation: We take corrective actions to address any damage caused by the breach, including restoring data from backups and implementing enhanced security measures. Following an incident, we conduct a thorough post-incident review to extract lessons learned and enhance our security protocols accordingly.

Improvement management

Processes and procedures are designed to prevent processing errors and non-conformities. The following processes and procedures collectively form our preventive action procedure designed to prevent the cause of potential non-conformities:

- Weakness escalation and review
- Communication and training
- Risk assessments
- Reviewing the ISMS
- Internal and external audits

NIPO maintains a Corrective/Preventative/Improvement actions list which outlines the nonconformity and subsequent results of action taken to correct it. This report is reviewed with management in efforts to understand progress towards continually improving our information security management system.

Update management

Nfield employs a robust update management strategy that leverages Microsoft Azure for server updates, ensuring a reliable and secure infrastructure. By utilizing Azure's automated update mechanisms, we maintain the latest security patches and enhancements for our servers, minimizing vulnerabilities. Our software is deployed using an agile approach, allowing for rapid and efficient updates in response to user feedback and evolving requirements. Each update undergoes a formal change management process to ensure that all modifications are documented, approved, and communicated effectively to relevant stakeholders. Comprehensive logs are maintained throughout the update cycle, providing a clear record of changes made, facilitating troubleshooting, and enhancing accountability in our development and deployment practices. This systematic approach ensures that Nfield remains secure, functional, and responsive to user needs.

7. Data retention and disposal

Data retention schedules (based on legal, business, and regulatory requirements)
Secure disposal of data (shredding, wiping drives, degaussing)

We store data no longer than necessary

Personal information will be retained only for such period as is appropriate for its intended and lawful use, in this case, we shall retain the data in accordance with our contractual commitment unless otherwise required to do so by law. Personal information that is no longer required will be disposed of in ways that ensure their confidential nature is not compromised.

As part of the Company Business Continuity plan and as required by ISO 27001:2022, and in certain circumstances the law, our electronic systems are backed up and archived. These archives are retained for a defined period in a strictly controlled environment. Once expired, the data is deleted, and the physical media destroyed to ensure the data is erased completely.

Nfield data retention

Upon termination of the agreement, NIPO will block and delete the customer data. During a period of 30 days following the termination of this agreement in whole, We can grant access to customer data during a 24-hour period in order to retrieve your data. Immediately after this 24-hour period, or when no access was requested after 30 days, NIPO will make any and all customer data inaccessible and delete the customer data.

8. Compliance with legal and regulatory requirements

GDPR, or other applicable regulations
Industry standards and certifications (e.g., ISO/IEC 27001)

Compliance with internationally recognized standards ensures that Nfield can offer our customers robust, secure, and reliable data management solutions. Through adherence to ISO/IEC 27001:2022 and GDPR, we support customers in maintaining trust and meeting regulatory requirements.

ISO/IEC 27001:2022 certification

Nfield is certified to ISO/IEC 27001:2022, the globally recognized standard for information security management. This certification demonstrates our commitment to securing customer data through stringent security protocols, including comprehensive policies for risk management, access control, data integrity, and incident response. Regular audits by independent third parties validate our compliance with these standards, ensuring that we maintain and continuously improve our security practices. With ISO/IEC 27001:2012 certification, Nfield upholds a structured approach to identifying and mitigating security risks, ensuring that customer data remains protected across our data collection platform.

The ISO 27001 certification operates on a three-year cycle, which includes annual surveillance audits. At the end of each three-year cycle, a re-certification audit is required to maintain the certification.

GDPR compliance and the Nfield GDPR Toolkit

As part of our commitment to data protection, Nfield fully complies with the General Data Protection Regulation (GDPR), the strict privacy regulation that governs the handling of personal data for EU residents. Our GDPR compliance program ensures that all data collected, processed, and stored by Nfield meets EU data privacy requirements, with transparent policies around data handling, consent management, and data access. To assist customers in their own GDPR compliance efforts, we offer the Nfield GDPR Toolkit, an essential resource with tools and guidance for GDPR-compliant data collection and management. This toolkit simplifies compliance by helping customers manage consent, securely handle sensitive data, and control data storage locations.

Nfield's rigorous approach to compliance with ISO/IEC 27001:2022 and GDPR empowers customers with a secure and compliant data collection platform, supporting operational confidence and regulatory assurance.

Privacy policy

NIPO has a privacy policy in place for all its websites, see our Nfield Manager privacy policy.

9. Auditing and monitoring

Regular audits (internal and external)
24/7 monitoring of systems
Log management and retention

ISO/IEC 27001:2022

ISO certification requires the organization to undergo periodic surveillance audits every year. In July 2025, the most recent and intensive 3-day re-certification audit was conducted which scrutinized both our Amsterdam and Madrid offices. Audit was performed by SGS.

Nfield Technical Security Assessment

In May and June 2024 Secura has conducted their annual Technical Security Assessment of the Nfield platform. The assessment included pen testing, black box and gray box tests. Crystal box testing is performed on a continuous basis at NIPO using external tooling (Veracode) against our build pipelines.

24/7 monitoring of systems

Continuous, around-the-clock observation of critical systems, applications, and infrastructure is in place for Nfield. This practice ensures real-time detection of issues, anomalies, or threats and enables rapid response to maintain uninterrupted service availability and optimal performance for customers. Customers can check system uptime on out Nfield Status portal.

Log management

When you work on Nfield your activities are automatically logged by the Nfield system. In this log we store almost every action a user does in the system. The log is available only to users in your organization who have an Nfield domain administrator role. It is there to allow the domain administrators to back-track why certain errors occur. When your account is deleted from the domain, the domain administrator will no longer know that you did an action; they will only be able to see that a deleted user did an action.

When your account is deleted in the Nfield domain, our software immediately deletes all personally identifiable information stored in the system and only an anonymous reference will remain for data integrity purposes. Because Nfield is backed up for no more than 4 days, any personal information about you that was deleted from a domain will be deleted fully from the Nfield servers after 4 days.

10. Employee training and best practices

Regular security training programs
Best practices for data handling

Continuous staff security training

Continuous security training for all NIPO staff is provided through:

- Kantar and Kantar security teams, also part of ISO 27001-2022 certification.
- Through Online training resources.
- Through NIPO's Premier Support contract with Microsoft

Processing of customer data

All NIPO staff are informed of the confidential nature of the customer data, they have received appropriate training on their responsibilities and have executed written confidentiality agreements. Only those personnel performing the services in accordance with the customer agreement shall have access to customer data, where this is considered strictly necessary for the performance of the services.

NIPO staff shall not delete, transfer, modify, extract, remove or otherwise process any of the customer data, except in accordance with the terms of the agreement.

Remote access

Inbound remote access is controlled through firewalled, encrypted Virtual Private Network (VPN) tunnels authenticated with two-factor authentication for those that require it in the course of their work.

Mobile device control

IT uses an industry leading, enterprise mobile device control console. Only authorized mobile devices that are centrally managed by the console are allowed to connect to the IT messaging systems. Mobile devices are required to comply with IT's mobile security policy that covers the device, provides for secure password control, allows remote wipe, forced wipe on device password lockout, and the devices are forced to be encrypted.

Physical Security

Access to office buildings is managed in conjunction with the relevant Facilities Management team. Where appropriate, information systems are restricted (isolated) only to those who require access in order to reduce the opportunity for unauthorized or unintentional modification, loss or destruction of information. Use of security badges and security monitoring are used throughout NIPO facilities. Visitors must sign in and be escorted throughout NIPO offices. This includes name and time of arrival and departure.

11. Third-party vendor management

Guidelines for working with third parties (security requirements, contracts)
Data protection requirements for external partners and suppliers
Monitoring and review of third-party security practices

To ensure the security of our information with third parties, we carefully select and manage our suppliers. Here's how we do it:

1. Choosing the right suppliers:
   Before signing any agreement, we assess potential suppliers based on their security practices and certifications. We prioritize suppliers with whom we share our commitment to data protection. We sign agreements which include commitments by the supplier on security practices and data protection obligations.
2. Ongoing monitoring:
   We regularly review our suppliers' performance and security measures. We stay updated on industry best practices and adjust our requirements accordingly.
3. Clear communication:
   We maintain open communication with our suppliers to address security concerns and share best practices. We work together to ensure the highest standards of information security.

By following these practices, we aim to protect your information and minimize potential risks.

12. Specific measures for Nfield CAPI

Tablet devices are desirable prizes for thieves. Their thin, lightweight nature also makes them easy to forget about and accidentally leave behind. Nfield therefore also deploys additional measures to limit the extent of data exposure risk due to being locally stored on a mobile device.

Minimal information

Nfield ensures the minimum amount of information possible is present on any mobile device at any given moment. Each device is only sent the surveys and associated respondent information specifically assigned to its user(s). Data that no longer needs to be accessible is removed as soon as possible.

You control which surveys and respondent details are assigned to each interviewer, so can limit exposure.

Survey response data is transferred to a local, encrypted database and removed from the device as soon as possible after each interview is completed. (As soon as the interviewer connects to internet network.)

Upon completion of each interviewer's involvement, all information relating to a project is deleted from their device as soon as you unassign them or close the project (once the interviewer has connected to the internet and synchronized their device with the Nfield system).

Secure device sharing

The same mobile device can be shared by multiple interviewers. Each survey and its collected data is only accessible to the relevant interviewer, via their login credentials. Interviewers cannot review, start or modify any surveys not specifically assigned to them.

Appendices

ISO certificate

ISO 27001 is an international standard for managing information security, and a must-have for any organization that is entrusted with large amounts of user data, as we are here at NIPO.

Since Nfield's inception in 2011, security and compliance have been core pillars of our platform. We secured our first ISO 27001 certification back in 2013, followed by rigorous annual audits.

We're thrilled to announce that SGS has confirmed our successful transition to the latest ISO 27001:2022 standard! This achievement is not just a milestone for NIPO; it directly benefits all Nfield users. We know this certification is increasingly vital for securing new projects, as clients demand assurance that their data is safe and secure. With Nfield, that assurance is guaranteed.

The 2022 standard represents a substantial upgrade from the previous 2013 version. Following last year's audit, our team immediately began preparing for this transition, which included a full re-certification. A massive thank you to the dedicated NIPO ISO Champions team for their fantastic work. Now, our business and our clients can truly benefit!

The validity of the ISO certificate can be checked here: https://www.sgs.com/en/certified-clients-and-products/verify-certificate?id=8d288c95-5220-4c5d-9947-bbe9655f78d9

See our latest ISO certificate on the right:

Certificate GB16/872164

The management system of

NIPO Software B.V.

Amsteldijk 166 1079 LH Amsterdam The Netherlands

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2022

For the following activities
The protection of information relating to the NIPO's development and delivery of Nfield SaaS survey platform which supports the professional market research industry. Core processes include: Design, Software Development, Product Management, Testing, Deployment, Platform Hosting and Support of the Nfield platform.
Assessed in accordance with the Statement of Applicability version 1.0 created 22 May 2025.

This certificate is valid from 17 July 2025 until 04 June 2027 and remains valid subject to satisfactory surveillance audits.
Issue 8. Certified since 30 September 2016

L. Moran

Authorised by
Liz Moran
Business Manager

SGS United Kingdom Ltd
Rossmore Business Park, Ellesmere Port, Cheshire, CH65 3EN, UK
t +44 (0)151 350-6666 - www.sgs.com

This document is an authentic electronic certificate for Client' business purposes use only. Printed version of the electronic certificate are permitted and will be considered as a copy. This document is issued by the Company subject to SGS General Conditions of certification services available on Terms and Conditions | SGS. Attention is drawn to the limitation of liability, indemnification and jurisdictional clauses contained therein. This document is copyright protected and any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful.

Page 1 / 1

Security assessment statement

This statement is provided to guarantee that Secura, a Bureau Veritas company (https://www.secura.com), upon the request of NIPO Software B.V. has conducted their annual Technical Security Assessment of the Nfield platform. Secura has been performing these assessments for NIPO Software B.V. since 2012.

Nfield is Kantar's destination platform. Next to wide usage in Kantar, the Nfield platform is also used by many market research companies across the world.

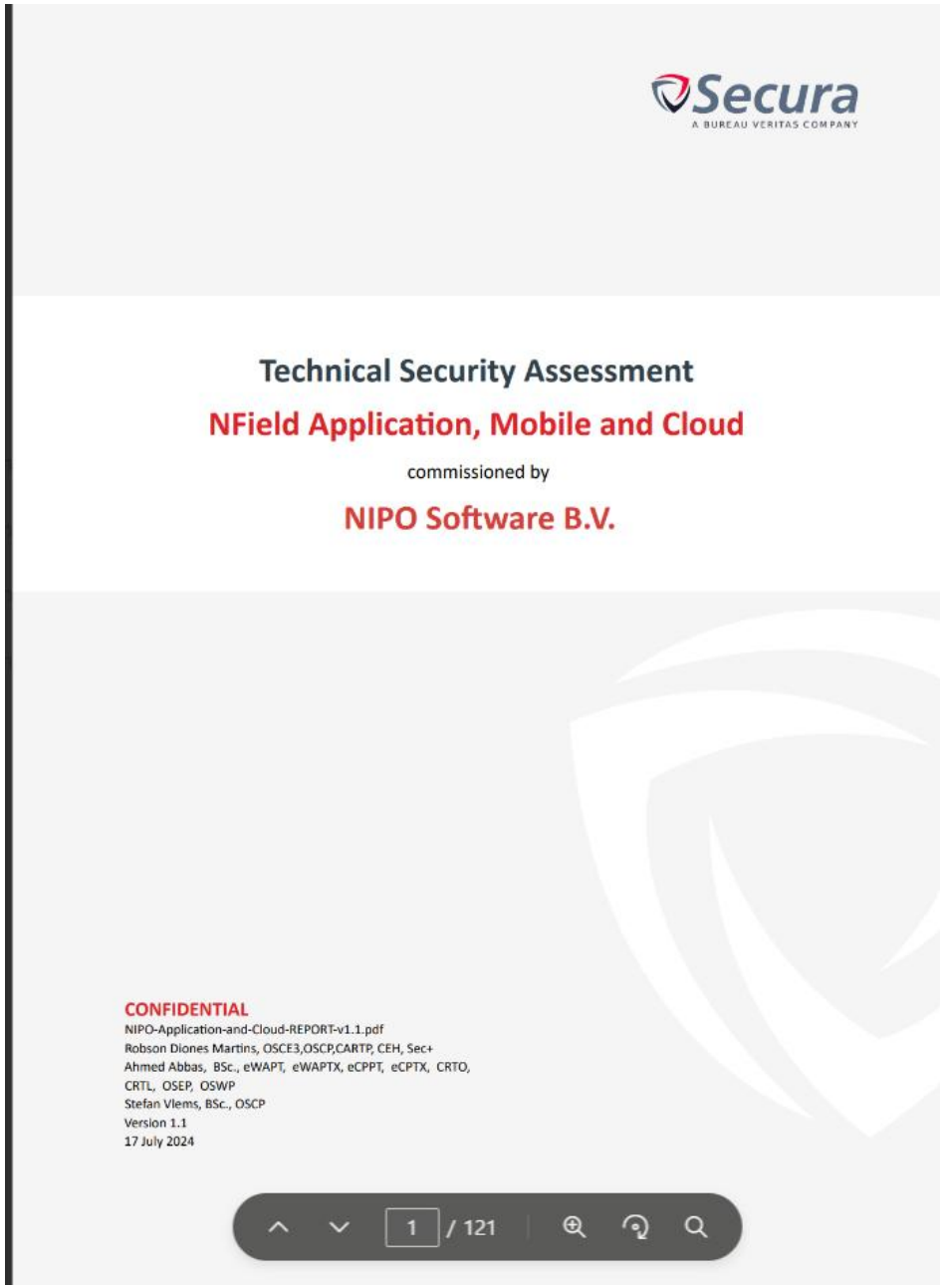
NIPO is a Kantar company.

The security assessment was performed over May and June 2024. The assessment included pen testing, black box and gray box tests. Crystal box testing is performed on a continuous basis at NIPO using external tooling (Veracode) against our build pipelines.

No critical, high or medium risks were identified by Secura.

Under current NDA, the Secura report has been shared with Kantar's Risk Assessment team.

Cover sheet of latest security report on the right:



NIPO
Amsteldijk 166
1079 LH Amsterdam
The Netherlands
sales@nipo.com

www.nipo.com