

New Zealand HISF (Suppliers) 2023

HISF Suppliers defines security and privacy requirements for protecting health information for New Zealand health agencies.



What it is

The New Zealand HISF Suppliers 2023 — Health Information Security Framework for Suppliers is a national security and compliance standard that supports organizations in managing cybersecurity risks and protecting health information when providing digital health services or products to the New Zealand health sector.

Published by Te Whatu Ora — Health New Zealand, the HISF Suppliers framework applies to all suppliers handling, processing, or storing health-related data on behalf of public health agencies. It addresses critical areas such as cybersecurity controls, privacy governance, risk management, and operational resilience, with a focus on aligning supplier practices with sector-wide compliance requirements for data protection.

At a glance

PUBLISHER Health Information Standards Organisation (HISO), Health New Zealand Te Whatu Ora	TYPE Framework	VERSION HISF Suppliers Guidance 2023
EFFECTIVE 2023	DOMAIN Supply Chain Security	FAMILY Other
REGION New Zealand	INDUSTRY Healthcare & Life Sciences	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.tewhatuora.govt.nz>

Why it matters

- **Strengthen cybersecurity governance** Enable systematic risk assessment and improvement of security practices across suppliers managing health information for New Zealand agencies.
- **Enhance regulatory alignment** Support alignment with national health data protection requirements and streamline compliance with contractual and statutory obligations.
- **Increase audit readiness** Facilitate evidence gathering and reporting processes, making it easier to demonstrate due diligence during audits or assessments.
- **Support third-party risk management** Provide a structured approach to assessing, monitoring, and managing supplier risks throughout engagement and operational lifecycles.

How SmartSuite supports NZ HISF (Suppliers) 2023

Supplier Security Control Framework

Structure HISF supplier requirements with ownership, scope, and implementation tracking.

Third-Party Risk Assessments and Due Diligence

Evaluate supplier security posture, onboarding assessments, and ongoing risk reviews.

Contractual and Compliance Obligations Tracking

Manage security clauses, compliance requirements, and supplier attestations.

Supplier Access Control

Track supplier access to health information and enforce least-privilege controls.

Incident and Breach Coordination Workflows

Manage supplier-related incidents, escalation processes, and communication protocols.

Supplier Monitoring and Compliance Reporting

Provide dashboards showing supplier risk posture, control coverage, and HISF compliance readiness.

Common framework mappings

CIS Controls v8.1

GDPR

HIPAA

ISO 27001:2022

ISO 27002:2022

ISO 27701

NIST CSF 2.0

SOC 2

Official resources

New Zealand Health Information Security Framework (HISF) for Suppliers

Defines security requirements for suppliers handling health information in New Zealand.
tewhatauora.govt.nz/our-health-system/digital-health/health-information-security-framework-hisf

HISF Implementation Guidance

Provides detailed guidance for implementing HISF requirements in supplier organizations.
tewhatauora.govt.nz/our-health-system/digital-health/health-information-security-framework-guidance

HISF Compliance Checklist

Outlines the compliance checklist for suppliers to meet HISF requirements effectively.
healthnz.govt.nz/health-professionals/guidance-standards/topic/digital-technologies/cyber-security-hub/health-security-frameworks

HISF Risk Management Framework

Describes risk management processes aligned with HISF security controls.
healthnz.govt.nz/health-professionals/guidance-standards/topic/digital-technologies/cyber-security-hub/health-security-frameworks

Frequently asked questions

What is the New Zealand HISF Suppliers framework used for?

The New Zealand HISF Suppliers framework is used to guide suppliers of digital health services in implementing cybersecurity measures and data protection controls when handling health information for the New Zealand health sector. It serves as a baseline for managing information security risks and ensuring suppliers align with health sector compliance standards.

Is compliance with the HISF Suppliers framework mandatory for organizations?

Yes, compliance with the HISF Suppliers framework is generally mandatory for suppliers engaged with public health agencies in New Zealand, as it is often incorporated into procurement and contractual requirements. It is not a certifiable standard like ISO 27001, but adherence is essential for supplier approval and ongoing engagement.

Who does the HISF Suppliers framework apply to?

The HISF Suppliers framework applies to all organizations and third-party suppliers that process, store, or manage health-related data on behalf of New Zealand public health agencies. This includes technology vendors, cloud service providers, and any organization with access to sensitive healthcare information.

What are the key requirements or controls in the HISF Suppliers framework?

The framework requires suppliers to implement controls across several domains, such as data privacy, access management, incident response, risk management, and supplier assurance. Key artifacts include risk assessments, evidence of control operation, policy documentation, and incident reporting procedures.

How is the HISF Suppliers framework implemented in practice?

Implementation involves integrating HISF controls into supplier onboarding, conducting security and privacy risk assessments, mapping contractual obligations, and establishing continuous monitoring for compliance. Suppliers are expected to operationalize documented security policies and routinely review control effectiveness.

How does the HISF Suppliers framework relate to other standards like ISO 27001 or NIST?

The HISF Suppliers framework is compatible with and references international standards such as ISO 27001 and the NIST Cybersecurity Framework. Organizations often align their security controls with HISF while leveraging broader frameworks to ensure comprehensive security governance and to meet multiple compliance requirements.

What are the ongoing compliance obligations under the HISF Suppliers framework?

Ongoing obligations include periodic compliance assessments, maintaining up-to-date risk registers, continual monitoring of security controls, timely incident reporting, and documenting evidence of ongoing control operation. Suppliers are also required to address any identified gaps or findings as part of continuous improvement efforts.

How would SmartSuite support New Zealand HISF Suppliers 2023 (Health Information Security Framework for Suppliers)?

SmartSuite enables organizations to manage the HISF Suppliers framework by providing risk tracking, control implementation management, and evidence collection capabilities. The platform supports compliance monitoring with dashboards and facilitates audit readiness by storing relevant documentation and records. It also streamlines reporting and remediation workflows, allowing for efficient oversight of both supplier performance and regulatory obligations.

License included / downloadable: Yes HISF supplier guidance is publicly available through New Zealand government health cybersecurity resources.

Full framework page and mappings: smartsuite.com/frameworks/new-zealand-hisf-suppliers-2023-health-information-security-framework-for-suppliers