

March 2024

Information Security Clauses

**Contents**

[Information Security Clauses Relevant for Healthcare Providers’ Suppliers 2](#_Toc1126751012)

[How to use these clauses 3](#_Toc1239374607)

[Core Clauses 3](#_Toc1303771363)

[Standards and Frameworks 4](#_Toc1285450524)

[Security Operations 4](#_Toc971082489)

[Data Security 5](#_Toc1508022277)

[Remote Access 6](#_Toc943979252)

[Supply Chain 6](#_Toc565046869)

[Software Security 7](#_Toc298255337)

# Information Security Clauses Relevant for Healthcare Providers’ Suppliers

This document provides a comprehensive list of information security clauses that may be incorporated into supplier contracts supplying information, data, systems, and related services to healthcare providers.

## How to use these clauses

Suppliers may include commercial vendors and/or healthcare providers providing systems and/or data services. While many suppliers will already have standard contract language when engaging with customers, there are key elements that healthcare providers should look for in these contracts or include in contracts which they develop themselves. You are advised to seek further legal advice on these clauses to ensure that these are fit for purpose and protect your organisational information, data, digital & healthcare systems.

The clauses are separated into relevant categories to assist healthcare providers when they are considering purchasing services and wish to contract with a level of confidence that the services ensure the confidentiality, integrity and availability of systems and information.

* [Core Clauses](#_Core_Clauses_that) – Clear legal, regulatory and liability accountability should be part of all contracting.
* [Standards and Frameworks](#_Cybersecurity_standards_and) - Compliance with security standards and frameworks provides the highest level of confidence and incorporates many of the security controls in the other sections of this document.
* [Security operations](#_Operational_security_clauses_1) - Shows suppliers have put in place ongoing activities for protecting information, detecting potential issues, and responding to incidents.
* [Data security](#_Data_Security_indicates) - Indicates the supplier is identifying information that is confidential and defining activities to reduce data breaches.
* [Remote Access](#Remote_Access) - Because remote access often extends cyber security risk factors, these security controls add an additional layer of security.
* [Supply Chain](#Supply_Chain) - Ensures the sub-contractors (supply ‘chain’) are required to follow commensurate cyber security practices.
* [Software security](#Software_Options) - Optional clauses for software suppliers.

### Core Clauses

Core clauses below should be considered as a minimum because they provide clear legal, regulatory and liability accountability and should be part of all contracting.

* **Overarching Security Requirements:** Supplier to address any reasonable specific security or cyber needs and requirements that <customer name> may have.
* **Cyber Insurance:** Requirement for Supplier to (at its own expense) procure and maintain cybersecurity insurance including network, electronic data, and privacy insurance. Such insurance should be in force from the commencement date and for the entire term. Supplier should be able to provide evidence to <customer name> that such cybersecurity insurance is in force.
* **Informing personnel:** Each party to ensure its personnel are aware of their confidential (and other security) obligations and do not disclose confidential information in an unauthorised manner. Supplier personnel are required to complete declarations of confidentiality and certifications of pre-employment checks as appropriate.

### Standards and Frameworks

The following cybersecurity standards and frameworks that are relevant to New Zealand healthcare providers and their suppliers should be part of service agreements. Objective proof that these standards and frameworks are being followed provides a high level of confidence when purchasing services.

The following clause is the minimum requirement that all IT suppliers should be included in contracts:

* **Security Frameworks:** Supplier will comply with the HISO 10029:2022 Health Information Security Framework and any other relevant Health Information Security Frameworks and standards, as notified and updated by the NZ Government.

The following clause is the minimum requirement for any critical infrastructure supplier (i.e., PMS system or laboratory supplier):

* **Security standards:** Compliance with all applicable security standards, including industry standards and specified international standards such as ISO 27001, ISAE3402, SOC, and ISO 22301 etc (or standards that are in addition to or substitute the standards mentioned above (i.e. where there are industry or international standards applicable that are not mentioned)).

The following clause is a gold standard requirement and suppliers should be working towards meeting this standard:

* **NZISM Standard:** Supplier to comply with the current version of the NZISM published by the Government Communications Security Bureau and other security requirements suggested by the NZ Government.

### Security Operations

Operational security clauses that show suppliers have put in place ongoing activities for protecting information, detecting potential issues, and responding to incidents.

Note: These functions are all included in the standards and frameworks listed above and are therefore duplicative if potential suppliers have already given evidence of securitycompliance in the previous section.

* **Security testing:** Supplier to ensure periodic security testing is conducted on <Product/s>. Where non-compliance is evident through security testing, there will suitable rectification, notification, and recovery provisions.
* **Encryption:** Requirement on Supplier to encrypt data and information according to the provisions regarding encryption keys (as well as access of those keys).
* **Protective technology:** Requirement on Supplier to implement and deploy the appropriate protective technology, such as intrusion detection at the network perimeter, URL filtering limiting web activity, and suitable DoS/DDoS (Denial of Service) protection.
* **Network security:** Supplier will develop as well as implement security configuration baselines for all endpoint and network device types that are utilised throughout the provision of services to <customer name>. The Supplier is also required to segregate its network into zones based on trust levels and control the flow of data traffic between zones.
* **Separation of environments:** Supplier will ensure that the development and testing environments for the software/services are separate from their production environments.
* **Monitor for vulnerabilities:** Supplier to monitor for vulnerabilities or issues that cannot be patched and implement the relevant controls for these vulnerabilities.
* **Viruses:** Supplier must notify any awareness or suspicion of viruses and take all actions necessary to eliminate and block any virus or restore most recent back-ups where necessary (all at its own expense), on top of other relevant preventative and mitigative measures.
* **Security updates:** Making sure that Supplier promptly implements security updates for software and services over time and where needed.
* **Security reporting:** Obligation on Supplier to provide periodic reporting on data quality and integrity.
* **Logging:** Supplier must meet applicable auditing and logging requirements such as maintaining a policy for managing system and data access logs, logging general activities and actions, logging key system and security events, and protecting logs from tapering or deletion. Logs should be retained for at least 2 years or as agreed and regularly reviewed.
* **Activities:** General requirement on Supplier to ensure operational activities are conducted in a manner where protection and security of confidential information, health information and otherwise personal information, is of the upmost importance.
* **Reviews and tests:** Supplier must implement security reviews and penetration tests if directed by <customer name>.
* **Risk management:** Supplier will establish a formal risk assessment process to identify security risks that may impact the services and/or software and mitigate such risks in a timely manner. The risk assessment process should involve identification of physical and environmental risks.
* **Background checks:** Supplier will conduct appropriate background checks on all new employees based on the sensitivity of the role they are being hired for, and the nature of the data and information they will be managing.
* **Back-ups:** Supplier must maintain and back-up all data in its possession.
* **Business Continuity/Disaster Recovery (BC/DR) plan:** Obligation on Supplier to implement a BC/DR plan to manage any data (or security) breach that may occur, including provisions relating to back-ups of data or information.

### [Data Security](#_Data_Security_indicates)

Data security indicates the supplier is identifying information that is confidential and defining activities to reduce data breaches. These functions are all covered in the standards and frameworks listed above.

* **Data storage:** All data from <customer name> should be kept secure, managed, protected, and only disclosed in accordance with General Security Requirements. In handling and storing data, Supplier should: ensure compliance with HISF; prevent unauthorised access, modification, or deletion; and implement suitable monitoring mechanisms.
* **Return of information:** All material and copies of information and data are to be returned to <customer name> (including all specifications, programs, source codes, and documentation) on expiry or termination of the agreement. Supplier must not retain any copies of any data or information, except where expressly permitted.
* **Data classification:** Supplier will develop, implement, and maintain a data classification scheme that is designed to ensure that data is classified and protected according to its respective confidentiality requirements.
* **Data anonymisation:** Requirement on Supplier to ensure that <customer name>’s data will not be used in the development or testing of new systems, services or software unless such data has been appropriately anonymised.
* **Data deletion and sanitisation:** Supplier upon termination or expiry of the agreement must sanitise or, if not possible, destroy where applicable all hardware relating to or storing Ministry data. If hardware is to be disposed of or destroyed, Supplier will ensure that all media/hardware that may be used to store, process, or transport such data is disposed of in a secure manner.

### Remote Access

Remote access security for suppliers. Because remote access often extends cyber security risk factors, these security controls add an additional layer of security when the healthcare provider feels they are required. Many of these controls are included in the standards and frameworks listed above, however more specificity is added to these statements below, if the healthcare provider wishes to include them in particular contracting situations.

* **Compliance with policies:** Supplier to comply with all remote access policies applicable.
* **Restrictions:** Remote access is only permitted and to be used for purposes of providing the services, such as diagnostics, upgrades, running the service, and maintenance. Any connection to <customer name> systems is only established for the time necessary as to provide that aspect of the services. Supplier must ensure any devices connected to remote access are protected from malicious software, and that all staff accessing are properly authorised.
* **Notification:** Immediate notification required when Supplier (and its personnel) become aware of any actual, suspected, or threatened breach of the remote access provisions. Right for <customer name> to suspend or withdraw access at any time it believes there may be such breach. Supplier to assist with mitigation, investigation and prosecution of such breach where required.
* **Updating access details:** Obligation on Supplier to ensure access details for authorised users are changed every three months or as otherwise whenever an authorised user leaves the Supplier. Immediate notification required when an authorised user no longer requires access to ensure the systems are not compromised in any way.
* **Indirect access:** Supplier will not use remote access or any other access to the system to indirectly access any other systems, computers, or networks, where access has not been granted by <customer name>.
* **Virtual Private Network (VPN):** Supplier should not solely rely on the availability of a VPN for remote access to provide services.
* **Acknowledgement:** Acknowledgement from both parties that remote access terms and conditions are necessary to maintain the confidence of staff, patients, and the public (including their health information).

### Supply Chain

Supply Chain Security: Much as the healthcare provider wishes to ensure their supplier is following appropriate cyber security practices, healthcare providers should ensure the sub-contractors (supply ‘chain’) are also required to follow commensurate cyber security practices. These functions are all covered in the standards and frameworks listed above.

* **Supply chain security assessments:** Supplier will conduct appropriate due diligence assessments of potential subcontractors or other third-party providers across the supply chain to assess whether they may impact the security of the services or software being supplied.
* **Third-party agreements:** Requirement on Supplier to ensure that agreements with subcontractors or other third-party providers contain the appropriate security requirements necessary to adequately secure the services and software being supplied.
* **Material storage**: Requirement for Supplier to keep and store Input Material and all other relevant material and equipment in safe custody and at its own risk. Supplier also to maintain good condition and not dispose of any materials supplied by <customer name>.
* **Material inventory:** Supplier will maintain an inventory of all hardware and software assets.

### Software Security

Optional clauses for software suppliers. Software products and services are often mission-critical and additional concerns for their ongoing use and support may be addressed in contracts to provide assurance to the healthcare provider.

* **Software warranties:** Requirement on Supplier to, upon installation, ensure that all software will be ready to be used in accordance with the applicable manuals and documentation, and that software will contain no viruses, spywares, trojan horses, or any other harmful code which could adversely affect<customer name>.
* **Software maintenance:** Requirement for Supplier to maintain sufficient resources, including software resources, and have an adequate program detailing such maintenance.
* **Software restraints:** Restriction on Supplier to only use tools, technology, or software that is referenced to and agreed, as well as in the manner specified, within the Agreement.
* **Software coding:** Supplier to ensure that all applications, software, and otherwise digital aspects of the services provided, are developed with secure coding practices. Supplier should consider Open Worldwide Application Security Project (OWASP) Top 10 Most Critical Web Application Security Risks when assessing whether secure coding practices have been used.