**Data sheet**

**Update to HISF Guidance for Suppliers**

This datasheet outlines the alterations made in the updated 2025 release of the [HISO 10029.4:2023 HISF Guidance for Suppliers](https://www.tewhatuora.govt.nz/publications/hiso-10029-42023-health-information-security-framework-guidance-for-suppliers).

|  |  |
| --- | --- |
| **Section/Requirement of HISF document** | **Update** |
| Purpose | Definition of suppliers was enhanced to include a broader aspect of the health sector. |
| Purpose | Reference to Secure Control Framework (SCF) and links were added. |
| HSUP08: Organisations have documented, approved, business continuity and disaster recovery management, operational resilience policies and procedures in place.    HSUP31: In the event of a disruption or failure, critical information or services are identified, and measures are taken for the continuity of services. | Added more details relating to Service Level Agreements (SLAs) |
| HSUP56: The lessons learned from business continuity and disaster recovery testing are reflected in the established and implemented information security controls. | Example of testing plan, including corrective actions for lessons learned. |
| HSUP32: Rules for effective use of cryptography, including encryption, and key management are defined and implemented. | Wording change to enhance the requirement for encryption for data at rest. |
| HSUP33: The complete lifecycle of the account(s) being used to access, process, or manage information and services is managed. | More examples relating to Role-Based Access Control and Privileged Account Management |
| HSUP34: User accounts are authenticated and circumventing the authentication process is prevented. | Clarification about the technical nature of these controls |
| HSUP35: Access to information and its associated assets is defined and authorised according to the business, customer, and security requirements by adhering to the organisation’s identity and access management policy or procedures. | Clarification about the business (administrative) nature of these controls (more about processes.) |
| HSUP36: Organisations are to ensure that only authorised users, software components and services are provided with privileged access rights. | Additional notes about third party risks and controls for this requirement. |
| HSUP62: The information processing systems, applications, devices, and services are synchronised to an approved time source. | Additional information about the requirement’s applicability to medical devices. |
| HSUP67: Suppliers are to be systematically evaluated, and their information security activities are reviewed before and after onboarding of their systems and services. | Requirement is new for the Guidance for Suppliers – it was already included in Medium-Large and Hospital guidance. |
| HSUP68: The organisation's information security requirements are to be included in the agreements with the suppliers. | Requirement is new for the Guidance for Suppliers – it was already included in Medium-Large and Hospital guidance. |