AuditDashboard

AuditDashboard

Privacy and security information

Audit New Zealand
Mana Arotake Aotearoa

AuditDashboard: Privacy and security information

This information sheet provides background on the security of transferring files for statutory audits. It is designed for your organisation's security, privacy and IT professionals.

The statutory audit process requires your employees to send many files to your audit team at Audit New Zealand. Your organisation may do this by e-mail, USB or through your own file sharing systems.

We are introducing a new tool to improve this process, called AuditDashboard. This is more than just a secure file transfer tool; it incorporates functionality that will make it easier for your employees to work with us. The status of requests for information, and tracking what files have been received, will be more transparent to all involved thanks to improved tracking and automated workflows. The system also allows the transfer of files that are too large to send by e-mail.

Trust and security

Protecting your data is of the utmost importance to us. AuditDashboard meets robust industry standards for privacy and security.

Controls:	Comprehensive, risk-based, information security program
Hosting:	Microsoft Azure's Australian Data Centres
Performance:	Active monitoring and automated scaling
Encryption:	All data, in transit and at rest, FIPS Compliant
Access control:	Advanced role-based access controls, with logging of all activity
Accreditations:	Independently assessed as SOC 2 Type 2 Compliant since 2016, with annual third-party penetration testing

Authority to Request data

We request information in order to complete the statutory audit of your organisation under sections 24 and 25 of the Public Audit Act 2001. These sections give us power to seek information that helps us carry out proper function (which in this case is the carrying out of the statutory audit). We are not changing the data we request, just the way that it is transferred to us.

Further information

If you have any questions, please contact your Appointed Auditor or Audit Manager in the first instance, who will direct your question to the appropriate person.

Frequently Asked Questions: General

Is the system secure?

Our top priority is ensuring your data is secure. This system is subject to independent reviews annually and has achieved compliance with internationally accepted security standards.

We have also performed our own assessment to identify the controls we would expect to be in place and ensure these are operating effectively. We have also engaged a New Zealand based security firm to review the work that we have done.

Where is the data being stored?

The data, along with all back-ups, will be stored in Microsoft Azure data centres in Australia.

Can you restrict access to specific employees?

Access is by invitation only from an existing user. Within the platform itself, sensitive or confidential data can be further restricted to specified users. This ensures data such as payroll information is only accessible by those in your organisation who should be able to see it.

How do you ensure nobody else will see my data?

Your organisation is set up as a client, and we then create restricted spaces within your client space for each audit visit. Specific auditors and users from your organisation are added to each specific space. Only authorised users will be able to see your data.

How long will you keep my data?

We expect to store the data for up to three years. This is based on our knowledge of what your team want, they tell us it is helpful to be able to access files that were sent to the audit team in previous years. On any termination of the contract with AuditDashboard, data will be deleted.

We already use a file transfer tool – can we keep using this?

Audit Dashboard is not just about the transfer of data. It also helps manage the audit process, improving the experience for your employees.

Does each employee using the system need their own account?

Yes, all of your staff who need to use the system should have their own account. We can set up as many of your employees as required.

If your employees should no longer need access to the system, due to a change in role or resignation, we will need your team to tell us or remove access themselves.

What about Te Tiriti o Waitangi and Māori Data Sovereignty?

We take our responsibilities to respect Te Tiriti o Waitangi and te ao Māori principles seriously and follow the Principles of Māori Data Sovereignty. Our review of the types of information we will request for the audit indicates there is a low likelihood of the data being tapu (sacred). If we require information that is tapu, we will not use AuditDashboard. If you need further information on this, please contact us.