New Zealand Society of Actuaries (Inc)

Data Security Policy

Overview

The New Zealand Society of Actuaries Incorporated (we, us, our, NZSA) handles sensitive data and information while undertaking our activities. We need to ensure that this data is protected from being lost or stolen. We must also ensure that users can access data for the Society to function effectively.

This policy sets out how we will collect, store, protect and dispose of data. It outlines who is responsible for what and how we handle any security incidents

Data

This section covers how we handle data safely and securely.

- What we collect
- Where we store it
- How we protect it

The NZSA has two different types of data:

1. **Member Information**

- WHAT IS COLLECTED: Name, Contact Details, Employer, Qualification Status, Interest Areas
- WHERE IT IS STORED: This is stored on the NZSA Website Server
- HOW IS IT PROTECTED: This data is protected by restricting access to it and ensuring the website provider has suitable security (see below).

2. **Council & Committee Minutes & Reports**

- WHAT IS COLLECTED: Minutes, Reports, Member Applications, Policies, Professional Standards, CPD Audit records and general information
- WHERE IT IS STORED: These are stored on the NZSA Google Drive and in Private and Employer Email and Network Servers
- HOW IS IT PROTECTED: This data is protected by restricting access to it and ensuring that users of this information understand the expectations placed on them (see below).

Systems

This section identifies the systems we have and the rules which govern them.

- What systems staff and volunteers can use
- How access to our systems is managed

The Society utilises three primary areas to store data and information:

1. **The NZSA Google Drive**

- WHAT IS STORED: This Google Drive is for use by Council Members, ONZL (as the Secretariat) and Committee Convenors. It is used to store Council and Committee files.

- WHO HAS ACCESS: Council Members should have access to all sub-folders in the drive. Committee Convenors should only have access to the sub-folders relevant to their committee and should not have access to any other NZSA folders.
  Only the President and Secretary should have access to the Complaints/Disciplinary proceedings folder.
- ACCESS MANAGEMENT: Access to this drive should be tightly controlled and reviewed by the Secretariat when membership of these groups' changes.

2. The NZSA Website Server

- WHAT IS STORED: The website is used to store all files and data relating to the NZSA website. The website contains NZSA members personal information. It is important that this information is held securely, and that the website security is appropriate to safeguard members information from potential cyber intrusions.
- WHO HAS ACCESS: Access to these files should be restricted to the Secretariat and the Website Editor(s).
- ACCESS MANAGEMENT: Access to the website should be reviewed by the Secretariat when the Editor or Secretariat staff change. This should include changing any access passwords.

3. Private and Employer E-mail and Network Servers

- WHAT IS STORED: Personal e-mail addresses are often used to transact NZSA activities. A wide range of data is stored on these services.
- WHO HAS ACCESS: The individual owner of the e-mail address/server. However, the provider of IT services will also have access.
- ACCESS MANAGEMENT: The use of private email and storage presents a risk to the NZSA. The NZSA does not have specific control over this data. It is important that volunteers and staff understand the responsibilities they have which are set out below to manage this risk.
- WHO SHOULD NOT USE: The President and Secretary should use the NZSA email addresses to transact NZSA business. In addition, any confidential matter or any email that has personal information should not be done on a private or employer email. This includes member complaints, low-income applications and CPD audits.

People and users

This section outlines our expectation for staff, volunteers and members.

- What their responsibilities are
- Things they need to report

1. Expectations

- That reasonable care is taken when handling or using NZSA data.
- Access passwords are secure (contain combinations of uppercase and lowercase letters, numbers and symbols. Passwords are changed frequently.
- NZSA data is stored on network drives only accessible only to you (i.e. shared drives are not used).
- When departing an employer, that any NZSA data that is needed is saved from the network server or shared with Council prior to departure. This is to ensure information is not lost.

- Critical files are backed up for preservation.
- That any members personal information is not held if the information is no longer needed.

2. Reporting

Council must be informed if any of the following occur:
- Data is lost or stolen.
- Data becomes unavailable due to a security intrusion, or a loss of access occurs.
- Accidental disclosure of NZSA data to third parties.
- A security breach occurs on the server where NZSA data is stored.

Problems and incidents

This section outlines our incident response plan which maps out what we will do during and after a security incident.

If the breach involves personal information, the NZSA Privacy Officer must be informed immediately. The Secretary is the current Privacy Officer.

The NZSA will need to follow the four key steps under the Privacy Act 2020: 1. Contain, 2. Assess, 3. Notify and 4. Prevent. Details can be found here:

In all other cases, the President is to be informed immediately. They will determine any remedial steps required to be taken, depending on the severity of the incident.

This policy and procedures are to be reviewed after any incident, or as part of the normal policy review cycle.

This policy was approved by Council on 18 April 2023

Scott Lewis

President

Matt Jensen

Secretary

New Zealand Society of Actuaries (Inc)