



Education Sector Authentication & Authorisation (ESAA) Code of Practice

VERSION: FINAL (April 2007)

© Ministry of Education, 2007

Table of Contents

1.	Introduction	2
1.1.	Purpose	2
1.2.	Who should read this document?	2
2.	Overview	3
3.	Contextual Framework	4
3.1.	Scope	4
3.2.	Components	4
3.3.	Compliance	4
3.4.	Statement of Limitation	5
3.5.	Basis of ESAA System Policy	5
4.	Trust	6
4.1.	ESAA Trust Level Relationship with EOI Confidence Levels	6
4.2.	Why an Organisation requires a Trust Level?	7
4.3.	Why an Application requires a Trust Level?	7
4.4.	Trusted Referees and the EOI process	7
4.5.	Authorisers & Access Control	7
4.6.	Role Provisioning	7
5.	Privacy	8
5.1.	Collection of Personal Information	8
5.2.	ESAA User-ID	8
5.3.	Retention of Personal Information	8
5.4.	Disclosure of personal information	8
6.	Security	9
6.1.	e-Gif Information Classification	9
6.2.	Overview of Security Architecture	9
6.3.	Operational and Network Security	9
6.4.	Identity based security	9
6.5.	ESAA System Administrator and ESAA Administrators (Helpdesk)	10
6.6.	Retention of EOI documentation	10
6.7.	User Security	10
6.8.	User Violation	10
6.9.	Change Control	10
6.10.	Compliance	10
7.	Management of the ESAA Environment	11
8.	Responsibility	13
8.1.	Application Owner's Responsibilities are to:	13
8.2.	Organisation's Responsibilities are to:	13
8.3.	Users Responsibilities are to:	13
9.	ESAA Stage 2	14
9.1.	Pilot Distribution model	14
9.2.	Pilot Federation model	14
9.3.	Government Logon Service (GLS) Integration	14
10.	Appendices	15
10.1.	Appendix A – Identity Roles	15
10.2.	Appendix B – Conditions of Use	17

1. Introduction

The vision of New Zealand's ICT Strategic Framework for Education¹ is *"to improve learner achievement in an innovative education sector, fully connected and supported by the smart use of ICT"*. The ESAA system is an open, standards-based solution, engineered to support a seamless link to the Education Sector online services, independent of the entry point into the sector networks.

The ESAA solution is an identity management system that enables user authentication, authorisation and single sign-on to online services. Users can log on to an online service with a single user name and password and traverse seamlessly between ESAA enabled applications without the need to log out of one application and repeat the log on process to access another application.

The Evidence of Identity process, assigning users a trust level appropriately aligned with the user's access requirements, is pivotal for the ESAA model to pave the way to Circles of Trust that effectively creates a virtual sector. Additionally, a common approach and acceptance of consistent security and privacy practices is essential across the spectrum of ESAA stakeholders.

Representatives from the Education Sector Agencies provide leadership to maintain sector and public trust in the security and management of electronic information, and aims to ultimately improve learner achievement.

The ESAA solution is the future model for the implementation of Circles of Trust via federated identities (the process of a user authentication across multiple organisations); thereby realizing the goal of a collaborative Australasian, and potentially, a wider community.

1.1. Purpose

Due to the diverse dimensions of the privacy, trust and security components impacting identity management, authentication and authorisation, it is necessary to establish a "shared zone of acceptance" around privacy and security practices.

The purpose of the ESAA Code of Practice is to introduce the trust, privacy and security principles necessary to develop a security conscious culture for organisations wishing to benefit from the ESAA service, and to provide an authoritative reference point for the management and related responsibilities of the ESAA service.

The ESAA Operations Policy further details the policies and standard practices to use the ESAA system to which stakeholders can align their support and commitment. A copy of the ESAA Operations Policy can be obtained from sector.servicedesk@minedu.govt.nz.

1.2. Who should read this document?

- The CEO, Principal, Vice-Chancellor (or equivalent) of an Organisation who desires to use the ESAA system and benefit from a single sign authentication service for users of ESAA enabled applications.
- Chief Information Officer
- Senior Business Managers

¹ www.minedu.govt.nz/goto/ictframework

2. Overview

The investment in Information and Communications Technology (ICT) is planned and co-ordinated through New Zealand's ICT Strategic Framework for Education (Strategic Framework). The objective of the Strategic Framework is to improve learner achievement through the smart use of ICT. The Strategic Framework is aligned with, and supports the e-Government and National Digital Strategies and the international e-Framework for Education and Research².

The Education Sector is moving from a model of relatively standalone education providers towards an ICT-enabled, networked, collaborative environment for learners, teachers, providers and agencies. The ESAA system is a key component of the Strategic Framework, as it addresses the fundamental issue of authentication. The ESAA system is an identity management, authentication, authorisation and single sign-on service. The ESAA system aligns the Education Sector with industry and government security protocols and shall support a seamless link to relevant Education Sector online applications, independent of the entry point into the sector networks – ultimately providing a secure, single sign-on for all Education Sector online applications.

The ability to transact seamlessly across the Education Sector with one logon (username) and password removes the need for users to repeatedly log in and out of various applications across the Education Sector using multiple password and user names. Additionally, the ESAA system allows self-provisioning for authorised applications, i.e. users shall be able to register themselves once and use this online registration process many times to access numerous applications across the Education Sector.

The facility of a single sign-on through the ESAA system will result in:

- Reduced time and inconvenience for users to complete transactions;
- Improved security and privacy through the reduction in use and re-use of passwords across online applications;
- Improve the flow of information among individuals, groups, government agencies and the Education Sector as whole.

The Education Sector has a legal and ethical obligation to ensure that privacy of individuals and the quality and integrity of electronic information is not compromised. Maintaining privacy and security of electronic information is compounded by the complexity and variety of stakeholders and systems involved. A Circle of Trust is established effectively to create a virtual sector, characterized by shared privacy and security principles, rules and expectations.

Compliance with the Code of Practice is required by all participants that use, or provide ESAA enabled services to:

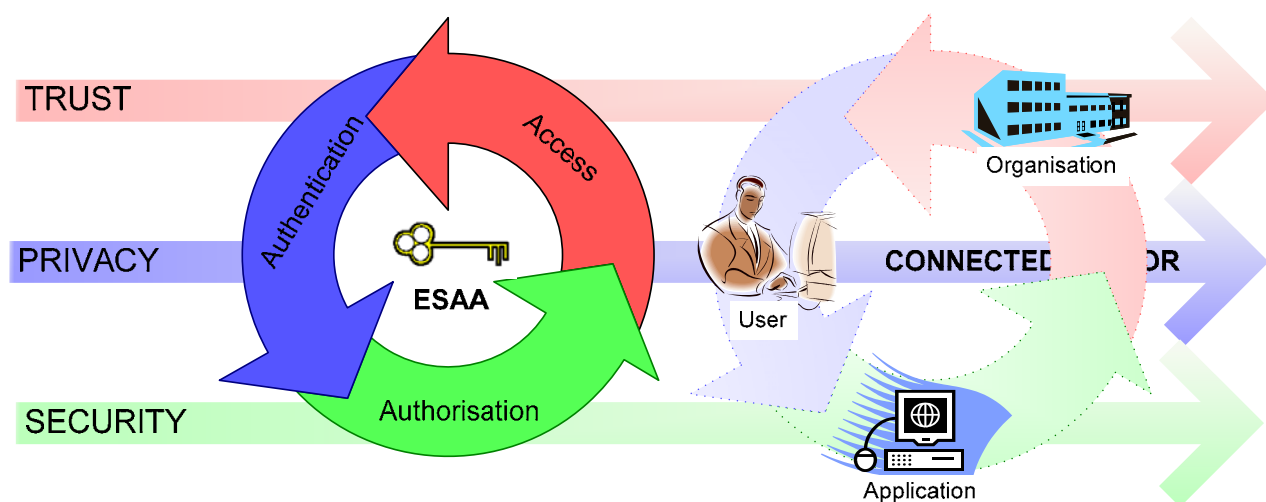
- Achieve private and secure access to online education resources;
- Enhance privacy and security collaboration between education providers;
- Provide the foundation to create a culture of privacy and security awareness.

² www.e.govt.nz/
www.digitalstrategy.govt.nz
www.e-framework.org

3. Contextual Framework

3.1. Scope

ESAA policy applies to all education providers and solution providers that interface with the ESAA system, and their respective users of ESAA enabled online applications. The principles of trust, privacy and security are key factors that build trustworthiness and a security conscious culture that protects the exchange of electronic information in the connected sector.



3.2. Components

Service providers are interpreted as the organisations that provide education and or an application.

ESAA stakeholders are...	Defined as....
Organisations	Government agencies and Education Providers (including schools, tertiary education organisations, ICT vendors, etc).
Application Owners	The individual responsible for the application and is located within a TEO, an agency or Education Provider.

Any one individual may at various times access online applications as any of the three categories of a user.

Users of the ESAA system are...	Defined as....
Agency employees	Employees of government agencies.
Sector employees	Education Sector users, generally those with administrative roles within schools and other education providers.
Other education sector participants	Learners or teachers who access information related to their studies either formal or informal.

3.3. Compliance

Compliance with the ESAA Code of Practice is required by those who provide ESAA enabled services and the users of these services.

3.4. Statement of Limitation

The architecture strategy for ESAA provides for three models for employing the identity management service (directory service);

- Centralised directory service – all users and their profiles shall be stored and managed within a centralised directory. Users shall be registered by a central administration team.
- Distributed directory service – an instance of the ESAA system is distributed across organisations. Users may be registered by administration teams within each organisation. User profiles shall be managed and stored within both a central (master) directory and distributed directories located at the organisation.
- Federated directory service – Each organisation shall operate its own identity management system (these need to be compliant with the ESAA supported international standards SAML2 and Shibboleth 1.3). Users shall be registered by administration teams within each agency. Each user shall have several profiles stored within directories of each organisation with which they have contact.

This document includes policy for the centralised directory service. It does not include policy applicable to ESAA distribution and federation models; these policies will be incorporated into ESAA stage 2 (refer to ESAA2 - section 10).

3.5. Basis of ESAA System Policy

ESAA Policy has incorporated and adopted policy and standard practices consistent with:

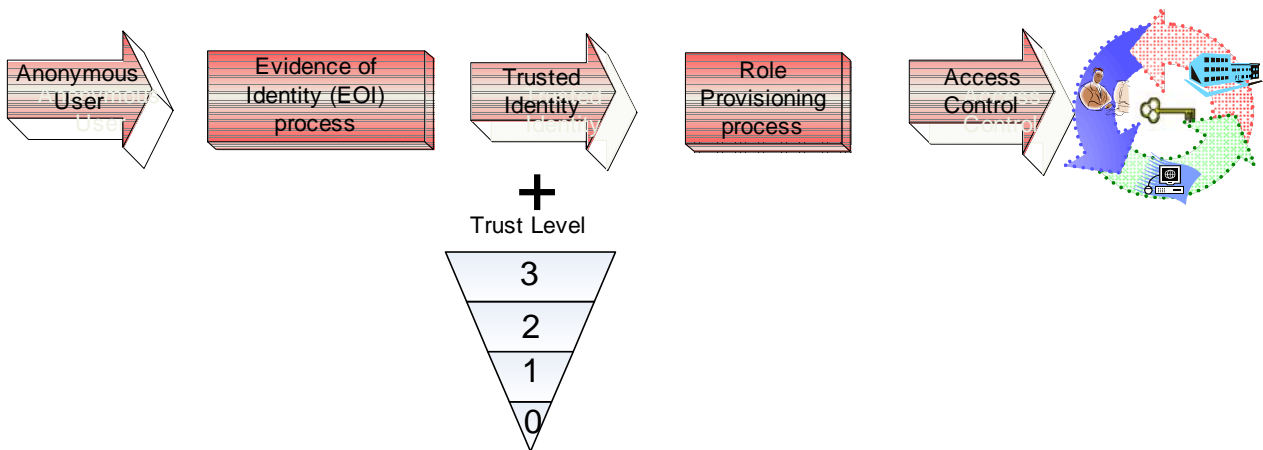
- Government legislation:
 - Privacy Act 1993
- Department of Internal Affairs (DIA)
 - Evidence of Identity Standard
The DIA is custodian of the Evidence of Identity standard, which outlines the approach to assessing identity-related risk that should be applied by New Zealand State Sector Agencies delivering services to the public
- State Services Commission
 - e-Gif – E-government Interoperability Framework – a collection of policies and standards endorsed for New Zealand government information technology (IT) systems
 - Guide to Authentication Standards for Online Services
 - Authentication Key Strengths Standard
 - Data Formats for Identity Records Standard

4. Trust

The principle of trust is built into the ESAA technology through the use of trust levels assigned to organisations, applications and users. By the members agreeing to comply with quality security and privacy practices, trust is strengthened, which achieves a standard necessary for a virtual sector to exist.

In order to authorise a new user access to an application, it is necessary to establish:

- Trust level for individual identities,
- Roles appropriate to the rights and privileges existing within an application.



An identity (a user or application) remains un-trusted until such time as they undergo a recognised Evidence of Identity (EOI) process i.e. one that is traceable, repeatable and auditable. The EOI requirements will depend on the level of confidence in the identity that is required for the particular service. A trust level between zero and three must be assigned to all registered users, applications, organisations and authorisers.

Access control is enforced through the establishment and definition of business roles, which have a minimum trust level. Role Provisioning is the process for assigning the user roles (permission types) within ESAA enabled applications.

4.1. ESAA Trust Level Relationship with EOI Confidence Levels

The level of identity-related risk is determined by analysing the range of consequences that can occur if access is given to an individual who claims an identity that is not their own. The table below illustrates the relationship between the risk category, Evidence of Identity (EOI) confidence levels and ESAA Trust levels.

Risk Category...	Evidence of Identity Confidence Level...	ESAA Trust Level...
Nil identity-related risk - referred to as 'anonymous' or pseudonymous' service.	<ul style="list-style-type: none"> • None required 	0
Low level of identity-related risk consequence in the service.	<ul style="list-style-type: none"> • Evidence of Identity is genuine and individual claiming identity uses it in the community. • Evidence of Identity accepted on 'face value'. 	1
Moderate level of identity-related risk consequence in the service.	<ul style="list-style-type: none"> • Evidence of Identity is genuine and individual claiming identity uses it in the community. • Individual is confirmed as the genuine claimant of the identity. • Evidence of Identity accepted on 'face value'. 	2

High level of identity-related risk consequence in the service.	<ul style="list-style-type: none"> • Evidence of Identity is genuine and individual claiming identity uses it in the community. • Individual is confirmed as the genuine claimant of the identity. • Evidence of Identity is verified by third party. 	3
---	--	---

4.2. Why an Organisation requires a Trust Level?

The Organisation's trust level determines the maximum trust level that can be assigned to their user. An Organisation's trust level is based on the strength of their EOI process.

4.3. Why an Application requires a Trust Level?

The trust level for an application is based on the sensitivity of the information held within the application, which dictates the user's minimum trust level necessary to access the application. The Application Owner determines the appropriate trust level based on a risk analysis of their application.

4.4. Trusted Referees and the EOI process

Trusted referees are a vital component of the EOI process. A Trusted Referee is a person who confirms that, to their knowledge; the presenting identity information corresponds to that individual and achieves the identity objectives for the associated trust level.

The CEO of the Organisation (or equivalent) is deemed a Trusted Referee and can appoint a suitable person to act as Trusted Referee for the EOI process, and as a point of contact should there be a discrepancy in the identity information supplied for the registration process. An internal trusted referee must undergo the EOI process to establish a level of trust in the ESAA system.

4.5. Authorisers & Access Control

In the ESAA environment there are three types of authorisers, the Application Owner, Access Authoriser and Role Authoriser. Authority begins with the Application Owner, who can nominate members of an organisation, suitable in rank, to act in the capacity as an Access Authoriser and/or Role Authoriser. Appendix A further details the Identity Roles in ESAA. It is the discretion of the Application Owner to set the authority level required for the application, i.e. Access Authoriser, Role Authoriser or no approval

4.6. Role Provisioning

Users must be provisioned with the appropriate business roles via the Access Authoriser or Role Authoriser for an ESAA enabled application, unless no approval is required. This will allow greater flexibility and control for users accessing ESAA-enabled applications and the information contained therein.

Type ...	Defined as....
Access rights	Lower level permissions, e.g. create, read, update, display.
Business roles	A defined role in the Education Sector, e.g. teacher, principal, comprised of a collection of functionalities, which are mapped to a person's job title.
Security roles	A group of access rights that are mapped to a specific functionality within an application.

5. Privacy

All information collected and retained within the ESAA system environment, either in hard copy or stored, is regarded as confidential and subject to the provisions of the Privacy Act. The design feature of the ESAA system allows all users to have one "identity" to access multiple applications, meaning only one set of personal data needs to be provided rather than multiple sets. This, along with the centralised storage of personal data, protects privacy.

The ESAA system collects the minimum personal information necessary to:

- Register an identity;
- Manage access;
- Audit and report incidences.

5.1. Collection of Personal Information

The EOI process shall gather the minimum information needed to establish the level of confidence required to mitigate risk associated with provision of the requested access to an application. A user's role is only activated in the ESAA system once their necessary personal information collected in the EOI process, is complete and accurate.

5.2. ESAA User-ID

Users are identified via a user-id, which is automatically generated and managed by the ESAA system. User-ids are only disabled after a significant period of inactivity.

5.3. Retention of Personal Information

Personal information is securely stored within the ESAA directory and requires authorised access to view and amend. Copies of EOI documentation, including electronic copies, are destroyed in a secure manner within two months of receipt.

5.4. Disclosure of personal information

Identity formation stored within the ESAA system shall not be disclosed to any person who is not a member of ESAA support or third parties, unless authorised to do so by the user or required by law.

6. Security

The principle of security encompasses the controls in place to safeguard Information and Communication Technology (ICT) and user's access to applications.

6.1. e-Gif Information Classification

Under the e-GIF information classification, all electronic information within the ESAA framework is deemed IN-CONFIDENCE special handling.

6.2. Overview of Security Architecture

Security Category...	Scope...	Responsibility...
Operational	Protect the MoE infrastructure supporting ESAA	MoE - Development Team
Network	Protect communication channels between the MoE and the organisations	MoE - Information Systems Group
Identity –based	Control access to information	MoE - Sector and Business Services Unit

6.3. Operational and Network Security

The ESAA system is housed at the Ministry of Education (MoE) and inherits the security controls and standards stipulated by the MoE Operational Security Policy, which is compliant with e-Gif and NZ Security in the Government Sector (SIGS) standards.

The security controls supporting the application is the responsibility of the organisation housing the application. The expected minimum is SIGS or NZ SIT 400, a supporting publication to SIGS is the Protective Security Manual, which provides implementation guidance³.

6.4. Identity based security

The ESAA system employs the following methods of identity-based security.

Method...	Scope...
User Provisioning	This is the initial registration of an identity in the ESAA system. An individual provides evidence to register their identity and gains an accepted trust level within the ESAA system.
Role Management	This is the entitlement or access privileges that an individual has for accessing a particular application, resource or information.
Authentication (key)	An individual is authenticated in the ESAA system at each login attempt when they have entered a valid username and password. Authentication information shall be protected during transit between the ESAA system and the application through channel encryption.
Authorisation	Access controls and policies are assigned to specific attributes or groups of attributes within the ESAA system using role-based control, which enable authorised access to specific online information, resources or services.

³ SIGS – www.security.govt.nz
NZ SIT 400 – www.qcsb.govt.nz

6.5. ESAA System Administrator and ESAA Administrators (Helpdesk)

Administrative access to ESAA infrastructure shall be restricted to those authorised individuals (system administrators) who are responsible for monitoring and or maintaining the ESAA system. ESAA Administrators are responsible for registration, provisioning of users and act as the first point of contact with the user for any ESAA system queries.

The concept of need-to-know, a security principle, states that the ESAA Administrator should have access only to information needed to perform a particular ESAA function, and shall be applied when evaluating authorisation rights and privileges.

6.6. Retention of EOI documentation

Copies of EOI documentation, including electronic copies, are securely retained only for the purposes of registering a new user or updating access levels for a current user in the ESAA system, before it is destroyed in a secure manner after two months from the date of receipt.

6.7. User Security

Security is quickly compromised through negligent behaviour of users, therefore organisations must ensure personnel are briefed and understand the responsibilities of using ESAA applications. The user is educated in the basics of security as detailed in the User Guide⁴ and the must accept the conditions of use when registering as a user of the ESAA system.

6.8. User Violation

The ESAA business owner reserves the right to monitor IT resources, including individual login sessions. Any violation of service use may constitute a breach of the conditions of use, which the user agreed to on registration, and action shall be taken appropriate to the seriousness of the breach. The Ministry of Education, Sector and Business Services (SaBS), is responsible for dealing with any violation of service use and shall liaise with the organisation's authoriser to ensure that appropriate action is taken.

6.9. Change Control

Any modifications to the ESAA system shall follow the change control process established for ICT shared services.

6.10. Compliance

Non-compliance with the ESAA Policy erodes the values of trust, privacy, and security necessary to achieve a connected sector. Organisations and ESAA enabled applications are subject to audit to ensure standards described in this code are adhered to.

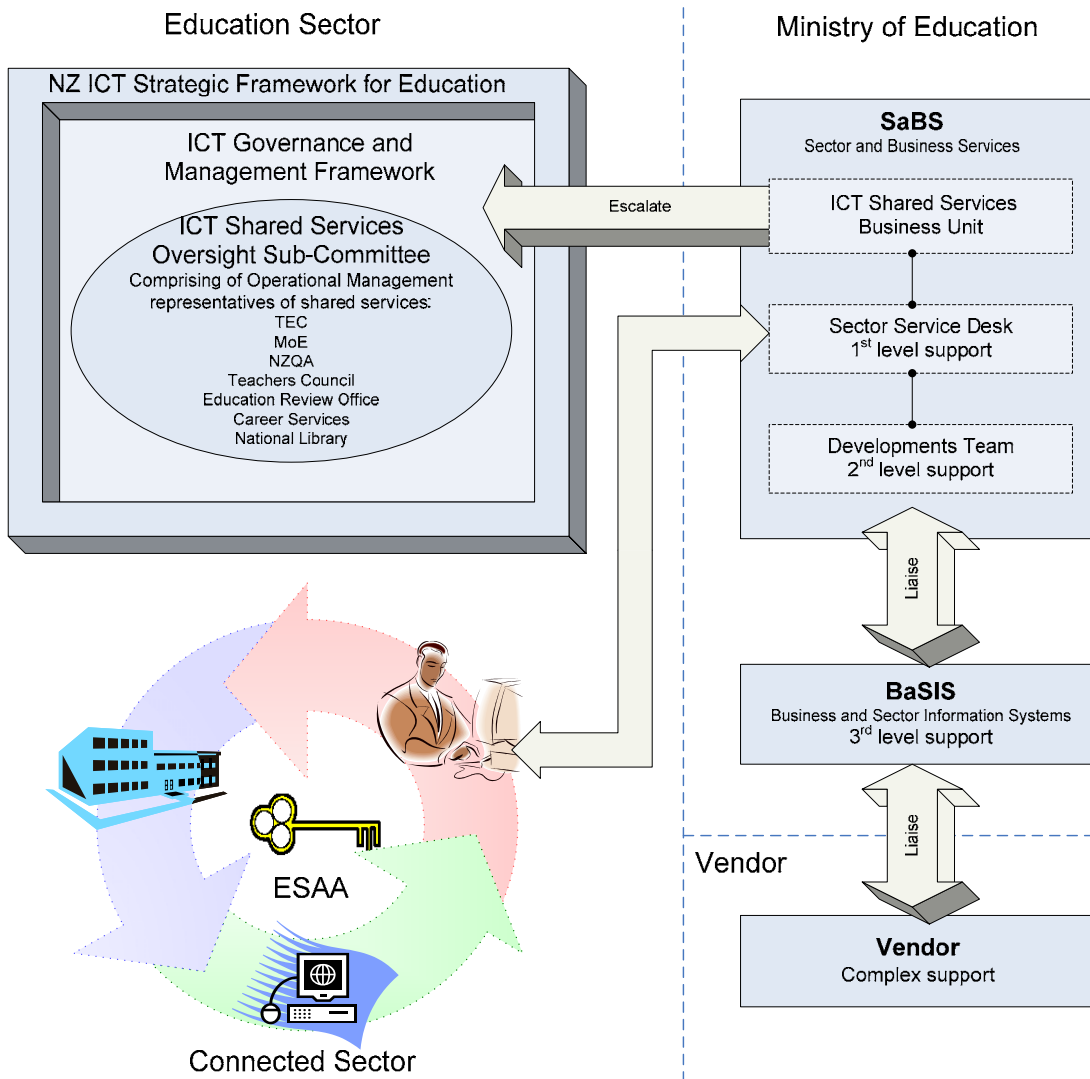
A full investigation shall be performed for any breach of privacy or security and reported to the Education Sector ICT Shared Services Oversight Sub-Committee.

⁴ www.steo.govt.nz

7. Management of the ESAA Environment

The ESAA system is a key component of the Education Sector Architecture Framework (ESAF) and the New Zealand ICT Strategic Framework for Education.

The diagram below illustrates the composition of the management, oversight and administration of ESAA environment.



Group...	Scope...
Education Sector ICT Shared Services Oversight Sub-Committee	<p>Oversight for ESAA environment is provided by members nominated from each of the Education Sector agencies, namely:</p> <ul style="list-style-type: none"> • Review and endorse any recommendations for new entrants (either organisations or new applications) that wish to utilise the ESAA service. • Provide an escalation point for any issues or risks that arise from the operational management of the ESAA system, including a breach to privacy and security policies.
MoE SaBS – Sector and Business Services	<p>MoE SaBS operates as the administrative arm of the Oversight Sub-Committee. Responsibilities include:</p> <ul style="list-style-type: none"> • Perform audit function of organisations and applications using the ESAA system to ensure identity security practices are compliant with the identity-based security outlined in Section 7. • Escalate any violation of privacy and security impacting ESAA's information and resources. • Evaluate and recommend proposed new entrants (either organisations or applications) that wish to utilise the ESAA service. • Provide first level technical support. • Administrate the EOI process for new users that wish to utilise the ESAA system. • Manage relationship with ESAA's vendor. • Escalate any violation of use of username and password impacting ESAA's information and resources.
MoE BaSIS – Business and Sector Information Systems	MoE BaSIS shall provide third level technical support.
Vendor	The vendor shall provide third level technical support.

8. Responsibility

The stakeholders in the ESAA environment must take responsibility to endorse and implement security and privacy policy and procedures for user provisioning, authentication, authorisation and access control.

8.1. Application Owner's Responsibilities are to:

- Ensure appropriate controls (manual and electronic) exist to ensure the integrity of electronic information that is stored and in transit.
- Ensure proper risk analysis performed to determine the authentication factors necessary to satisfy the trust level required for the application.
- Nominate an authoriser to perform the duties of Access Authoriser, Role Authoriser and Trusted Referee defined in the EOI process.
- Perform regular audits to ensure that privacy and security controls are in place over their application that satisfies the standards of the privacy and security policies.
- Ensure that staff understand and comply with security requirements.
- Liaise with the Sector Service Desk.
- Ensure that the standards of use for their application are understood, and enforced through an agreement with the user.

8.2. Organisation's Responsibilities are to:

- Ensure the ESAA EOI process is followed.
- Ensure secure storage of EOI personal information.
- Satisfy the criteria around the various roles of an Authoriser, and ensure that they are aware of their duties.
- Ensure that access rights and privileges granted to a user align with their purpose for accessing online applications.
- Perform regular audits to ensure satisfactory privacy and security controls are in place.
- Ensure that staff understand and comply with security requirements.
- Liaise with the Sector Service Desk.

8.3. Users Responsibilities are to:

- Complete the EOI process to become a trusted identity in the ESAA system.
- Receive appropriate authorisation for access levels.
- Acknowledge and accept conditions to use ESAA enabled applications described in the User Guide.
- Follow password construction and management rules.
- Follow password and access rules.

9. ESAA Stage 2

ESAA Stage 2 shall leverage users, processes and technology instigated in ESAA Stage 1 to achieve the education agencies' long-term vision of "improving learner achievement in an innovative education sector, fully connected and supported by the smart use of ICT".

Education sector agencies shall further support the shift towards this vision by piloting Circles of Trust and federated identity across the Education Sector. Distributed instances of the ESAA system and Federation allow various parties and their identity infrastructures to interoperate.

9.1. *Pilot Distribution model*

Distribution architecture permits both centralised and localised components of the ESAA service directory. Each organisation shall have access to both local applications and centralised ESAA applications for administration and reporting.

9.2. *Pilot Federation model*

Federation architecture shall provide access control in situations where the user's identity is not asserted by the ESAA system itself. It is anticipated that the ESAA service shall need to federate using federated protocols such as Shibboleth and/or SAML (Security Assertion Markup Language). Shibboleth, a project of Internet2/MACE, is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls.

9.3. *Government Logon Service (GLS) Integration*

Integration of the ESAA system with GLS provides users a single point of entry to online government services.

Federation introduces new security challenges and ESAA Code of Practice shall be modified accordingly.

10. Appendices

10.1. Appendix A – Identity Roles

Identities Involved...	Defined as...	Criteria ...	Rights...
Applicant	A person applying for an initial or increased ESAA trust level role rights.	<ul style="list-style-type: none"> • An employee of an education provider. • A user of online services. • Identity established at the respective education provider. 	No rights
User	The set of people and organisations registered and authenticated to use online services.	<ul style="list-style-type: none"> • An employee of an education provider. • A user of online services. • Identity established at the respective education provider. 	Access application per trust level assigned in the EOI process.
ESAA Administrator Sector Service Desk – 1 st level support & team lead.	First level support for all ESAA system users.	<ul style="list-style-type: none"> • Employed within the Sector Service Desk – MoE. 	<ul style="list-style-type: none"> • Set up user account in the ESAA system; • Assign and activate trust level in the ESAA system; • Role provision in the ESAA system.
ESAA System Administrator	Second level support for all ESAA system users. One who can perform all functions within the ESAA system.	<ul style="list-style-type: none"> • Employed within the Sector Service Desk – MoE. 	Super-user functions in the ESAA system.
Trusted Referee (1)	<ul style="list-style-type: none"> • The Organisation's CEO. • A trusted identity who has been assigned authority as a Trusted Referee to confirm and verify EOI documentation within their organisation by their organisation's CEO. 	<ul style="list-style-type: none"> • Authenticated to trust level 2 and above. • Must work for a Trusted Identity Provider. • Must work for the same organisation as the person whose identity they are confirming (except for ESAA Admin staff) 	Authorise trust levels limited to their organisation's trust level.
Trusted Referee (2)	A Trusted Referee who is external to an organisation i.e. registered accountant, Justice of the Peace, Doctor, Lawyer, Board of Trustees Chairperson, School Principal, Minister of Religion, Kaumatua.	<ul style="list-style-type: none"> • Must not be related or a partner/spouse of the applicant or residing at the same address. • Must be a registered professional with an accessible contact address and phone number. 	Validate identity.

Continue...

Identities Involved...	Defined as...	Criteria ...	Rights...
Role Authoriser	A trusted identity who has been assigned specific authority as a role authoriser in the context of their own organisation by an Access Authoriser or Application Owner.	<ul style="list-style-type: none"> ● Authenticated to trust level 2 . ● Must work for a trusted organisation that is at Trust Level 2 or higher. 	Authorise role requests for their organisation.
Access Authoriser	A trusted identity who has been assigned specific authority of an Access Authoriser by the Application Owner.	<ul style="list-style-type: none"> ● Authenticated to trust level 2. ● Must work for a trusted organisation that is at Trust Level 2 or higher. 	<ul style="list-style-type: none"> ● Request new security and business roles; ● Authorise role requests; ● Nominate and authorise a Role Authoriser across organisations; ● Authorise Role Authoriser rights for organisations.
Application	An online service.	<ul style="list-style-type: none"> ● Education Sector online service. ● Security criteria are satisfied as defined in the Security Policy. ● Trust level assigned based on risk analysis by Application Owner. 	N/A
Application Owner	An Access Authoriser who has been identified as the owner of an application.	Deemed application owner	<ul style="list-style-type: none"> ● Perform risk analysis to determine the trust level for their application. ● Request new security and business roles; ● Authorise access to all users (regardless of the organisation they belong to); ● Delegate the role of an Access Authoriser or Role Authoriser roles.
Organisation	<ul style="list-style-type: none"> ● Government Agency, Tertiary Education Organisation and Education Providers. ● The organisation that supplies online services. 	Provider of online services.	N/A

10.2. Appendix B – Conditions of Use

Below are the Conditions of Use described in Section 4 of the User Guide⁵.

These conditions of use apply to your accessing Education Sector online services. Please read them before signing the Acceptance of Conditions for ESAA. You are responsible for reviewing these conditions, and on accessing any Education Sector online service, you are deemed to have agreed to these conditions.

Security

You are responsible for ensuring that you use your access to ESAA enabled services in a manner which does not contravene theirs, or ESAA's security policies. Further, you agree that you will:

- Take all reasonable steps to prevent someone misusing or gaining unauthorised access to your computer system.
- Ensure your computer system has appropriate anti virus software installed.

Privacy

ESAA complies with the Privacy Act 1993 and is committed to respecting the personal privacy of individuals who use Education Sector online services. You agree:

- We can collect information about the ways in which you use ESAA. We will ask you for this information or we will obtain it from our records.
- All information you give is correct and complete.
- We may monitor / record calls made between you and the Tertiary helpline to maintain and improve the quality of ESAA.

You may ask to see information that we have about you and you may ask us to correct any errors. We will hold the information securely and will not disclose it to any person or organisation without your authority, unless required or authorised to do so by law.

Disclaimer

The Education Sector, while making reasonable efforts to ensure the accuracy and completeness of information and material, assumes no responsibility for the accuracy, reliability or completeness of that information or material. In addition, the Education Sector is entitled at any time, without prior notice, to change the conditions of use for accessing online services.

Your Responsibilities

You have an important role to play in the secure use of online services. You are responsible for your own behaviour when accessing online services. The following outlines rules and recommendations for online service use, password construction and management and challenge response guidelines.

General Use

- You must not send frivolous, obscene or defamatory messages.
- You must not look at, change, delete or tamper with files or programmes that you are not authorised to access.

Passwords

A password within ESAA must:

- Have a minimum of 7 characters, and
- Contain 3 of the following – Lowercase, Uppercase, Digits, Punctuation, and Special character.
- Be changed regularly.
- Be easily remembered, but difficult to guess.

You must not:

- Write passwords on sticky notes, desk pads, calendars, or store online.
- Share your user name and password with another person.

⁵ www.steo.govt.nz

Challenge Responses

The first time you logon to Education Sector online services you are required to set challenge response questions and answers. Challenge responses allow you to uniquely identify yourself and change your own password online should you forget it.

You must not:

- Reveal your password or challenge response answers to any other person.

You will never be asked for your password or challenge response answers by a legitimate ESAA administrator.

Breach of Conditions of Use

Any breach of the conditions of use, which you signed to on registration, will be dealt with appropriate to the seriousness of the breach.

Access to online services will normally be revoked during this investigative period and each incident will be considered on a case-by-case basis.

Minors

If you are under 18 you are encouraged to seek advice before accepting these conditions. Please do not accept these conditions if you do not understand any part of them.

These conditions are considered to be fair and reasonable. Should any of the conditions of use not be considered 'fair and reasonable', the condition will be reviewed and possibly amended to reflect the original intention.

In some circumstances the parents, legal guardians or employer of minors (those under 18 years of age) will also be asked to sign the Acceptance of Conditions of Use alongside the person wishing to have access to online services. The parent, legal guardian or employer of the minor, will then also be responsible for ensuring that the conditions of use are adhered to.