Information Security Management Policy

Printed Saturday, August 06, 2022
Live Document: https://staff.etoolglobal.com/?p=13787

Contents

- 1 Purpose
- 2 Scope
- 3 Relevant Issues
- 4 Interested Parties
- 5 Policy Statement
- 6 Objectives
- 7 Roles
- 8 Responsibilities
    - 8.1 Compliance, monitoring and review
    - 8.2 Records management
- 9 Information Asset Register
- 10 Statement of Applicability
- 11 Information Classification at eTool
- 12 Related Legislation
- 13 Related Procedures and Documents
- 14 Feedback
- 15 Document History

Purpose

The purpose of this policy is to:

- Clearly define the meaning of “information security” at eTool
- Outline the relevant issues and interested parties relating to information security at eTool
- Communicate eTool’s commitment to information security both internally and externally

Scope

This policy outlines how eTool manages information security.

Relevant Issues

Internal

- **Our reputation:** Poor management of information security by eTool is likely to impact our reputation poorly as stakeholders lose trust in our business
- **Our Mission:** Poor management of information security by eTool is likely to indirectly impact the effectiveness of our business in delivering it's mission of improving the environmental performance of the built form (e.g. losing customers due to reputation damage reduces the carbon out platforms can save)
- **Our growth:** Poor information security management will likely hamper our growth due to reputation damage
- **Legal and Social License to Operate:** Poor management of information security by eTool could lead to loss of our legal or social license to operate
- **Staff and Candidates:** Poor management of information security (particularly resume and recruitment information) by eTool could lead to loss of ability to retain and attract staff
- **Financial Risk:** Poor information security by eTool may result in direct financial losses for eTool

External

- **Customer's reputations:** Poor information security by eTool may impact our customer's reputations if their customer's data is lost
- **Legal and Social License to Operate:** Poor management of information security by eTool could lead to loss of our customer's legal or social license to operate
- **Environmental and economic losses:** Poor information security by eTool that affects our growth will lead to slower or more expensive decarbonisation of the economy
- **Customer Financial Risk:** Poor information security (particularly credit card details) by eTool may result in financial losses for customers

Interested Parties

- **Community:** The community relies on our success to help stabilise the climate and restore balance between the economy and the biosphere.
- **Customers:** Our customers rely on our management of information security to maintain their reputation and license to operate.
- **Staff:** Our staff rely on our management of information security to ensure their personal and sensitive information is safe
- **Shareholders:** Our shareholders rely on our management of information security for altruistic reasons (they have invested in eTool to help the planet) and financial reasons (they would like a return on their investment)
- **Industry Bodies:** Industry bodies rely on eTool's continued license to operate to deliver affordable, accurate and effective services and software to improve the environmental performance of the built form.
- **Governments:** Increasingly governments will rely on Life Cycle Assessment and eTool to deliver deliver affordable, accurate and effective services and software to improve the environmental performance of the built form.

Interested parties are also featured on our org chart.

Policy Statement

eTool is committed to adequately managing risks relating to Information Security and ensuring adequate controls are in place to mitigate unacceptable risks. Management at eTool will lead by example in their commitment to Information Security. eTool will maintain an Information Security Officer responsible for coordinating all

activities related to information security management.

Objectives

Zero harm from security related incidents is the over-arching objective of our Information Security Management System

We will achieve this by:

- Maintaining appropriate Information Security Policies (Information Security Officer)
- Maintaining appropriate records, procedures, management strategies etc to support information security (Information Security Officer)
- Ensuring our staff and contractors are appropriately vetted and legally bound to protect information security (Chief People Officer)
- Ensuring our staff and contractors are provided with appropriate training and that staff undertake that training to protect information security (All Staff, Chief People Officer, Information Security Officer)
- Maintain an Information Asset Register of both digital and physical devices in order to support information security (Information Security Officer)
- Adequately control access to information assets (All Staff, Information Security Officer)
- Adequately implement cryptography to support information security (All Staff, Product Team, Information Security Officer)
- Maintain physical and environmental security in a manner that adequately mitigates security risks (Office Managers, Information Security Officer)
- Ensure that all relevant activities in the business, be they regular or rare, recurring or singular are managed in a manner that ensures information security (All Staff, Group Managers, Information Security Officer)
- Ensure that electronic communications, networking, messaging etc are adequately controlled to protect information security (Product Team, Information Security Officer)
- Ensure that suppliers are adequately assessed in relation to information security
- Ensure that security incidents, be they actual or “near misses” are documented, investigated and appropriately actioned to avoid re-occurence (All staff, Information Security Officer)
- Maintain business continuity procedures and systems to manage information continuity and ongoing security of information during adverse / crisis events (All Staff, Information Security Officer)

Roles

The current Information Security Officer is the Managing Director of eTool Pty Ltd t/a Cerclos.

Responsibilities

Compliance, monitoring and review

Responsibility	Description	Who
Compliance	Following the policy	All staff
Monitoring	Ensuring the compliance with the procedure or policy	MD and Senior Management
Review	Reviewing the procedure or policy to ensure it is kept up to date	Information Security Officer

Reporting	Reporting requirements of the policy and procedure (for example statutory reporting responsibilities)	Information Security Officer

Records management

Staff must support the Information Security Officer in maintaining all records relevant to administering this policy in an approved company format and location.

Information Asset Register

eTool's Information Asset Register is located here. New information assets must be added to the Information Asset Register and associated risks added to the business risk and action register.

Statement of Applicability

eTool's ISO 27001 Statement of Applicability is documented here.

Information Classification at eTool

- **Public data:** Data that eTool has been given explicit permission to share publicly.
- **Internal data:** All employees and contractors who have signed an NDA have unrestricted access.
- **Restricted data:** Relevant employees and contractors who have signed an NDA or are adequately constrained under their employment contract may access data if:
    - The person has completed security awareness training and read this policy AND
    - Their role is specifically approved for access to that data, or they have written permission from the Information Security Officer or the data owner.
- **Confidential data:** Customer data, financial data, human resources data etc that eTool has implicitly or explicitly committed to keeping confidential. Relevant employees and contractors who have signed an NDA or are adequately constrained under their employment contract may access data if:
    - The person has completed security awareness training and read this policy AND
    - Their role is specifically approved for access to that data, or they have written permission from the Information Security Officer or the data owner.
- **Personal data:** Names, addresses, phone numbers and other personal information. Relevant employees and contractors who have signed an NDA or are adequately constrained under their employment contract may access data if:
    - The Information Security Officer has reviewed the person's personal security audit to ensure adequate understanding and compliance with basic security measures AND
    - The person has completed security awareness training and read this policy AND
    - Their role is specifically approved for access to that data, or they have written permission from the Information Security Officer or the data owner.
- **Sensitive data:** Personal data that also includes information about people including racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sexual orientation. Resumes may include sensitive data that could be used to gather information and discriminate against people. Relevant employees and contractors who have signed an NDA or are adequately constrained under their employment contract may access data if:
    - The Information Security Officer has reviewed the person's personal security audit to ensure

adequate understanding and compliance with basic security measures AND
- The person has completed security awareness training AND
- The person has completed Advanced Security Training 1 – Fundamentals of Cyber AND
- The person has completed Advanced Security Training 2 – Anatomy of a Hack AND
- The person has completed Advanced Security Training 3 – Understand the Threat AND
- The person has read this policy AND
- Their role is specifically approved for access to that data, or they have written permission from the Information Security Officer or the data owner.

Related Legislation

EU – General Data Protection Regulations

UK – Data Protection Act

Australia – The Privacy Act

New Zealand – Privacy Act

Related Procedures and Documents

Information Security Documents:

Personal and Sensitive Data Protection Policy

Security Awareness Training

Data Breach Response Plan

Advanced Security Training 1 – Fundamentals of Cyber

Advanced Security Training 2 – Anatomy of a Hack

Advanced Security Training 3 – Understand the Threat

Password Management Policy

Acceptable Use Policy

Supporting Documents

Quality Management Policy

Risk Management Procedure

Risk Management Training

eToolLCD Development and Deployment Procedure

eToolLCD Disaster recovery plan

eToolLCD Software Version Control

Feedback

Staff may provide feedback regarding this policy by contacting the authors directly or publicly posting a comment on the policy page.

Document History

Approval and Amendment History

Version	Date	Authors	Approved By	Comments
1	5th August 2022	Richard Haynes	Henrique Mendonça	First Version
2	4th October 2022	Richard Haynes	Sarah Megara	Amendments based on Information Security Management Review – 2022
3				