ICDL

The Digital Skills Standard

Information Security Policy

Contents

Overview

ICDL Foundation ("ICDL") is committed to upholding the highest standards of information security to protect the integrity, confidentiality, and availability of data within our software platforms and certification services.

With 17,000,000+ candidates, 20,000+ Test Centres, and a presence in over 100 territories, operating in 40+ languages, information security remains paramount across our global operations.

This Information Security Policy serves as the framework for our Information Security Management System (ISMS), aligning with the ISO 27001 standard requirements.

Scope

This policy applies to all employees, contractors and third parties involved in the development, delivery, and support of ICDL's software platforms and certification services.

It encompasses all aspects of information processing, storage, transmission, and disposal within ICDL.

When we refer to assets, or data assets, in this policy we are referring to the application and/or devices that stores data for ICDL, and the data itself.

Information Security Objectives

Aligned with ISO 27001, our information security objectives are set, reviewed and monitored regularly by the ISMS Team. These are designed to ensure the ISMS delivers on the following core objectives:

- Safeguard the confidentiality, integrity, and availability of data assets.
- Identify, assess, and mitigate information security risks systematically.
- Implement appropriate controls to address identified risks effectively.
- Continuously enhance the ISMS to adapt to evolving threats and organisational needs.
- Promote a culture of security awareness and responsibility among all stakeholders.

Risk Assessment and Treatment

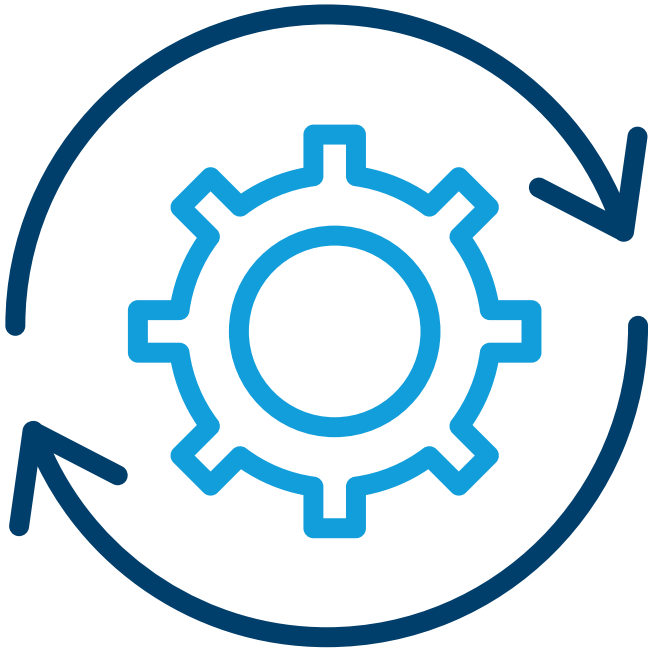
ICDL undertake a systematic approach to identifying, assessing, and managing information security risks in accordance with ISO 27001. This includes:

- **Identifying and evaluating information assets and associated risks.**
- **Determine the likelihood and impact of identified risks.**
- **Implement controls to mitigate or manage risks effectively.**
- **Periodically review and update risk assessments to reflect changes in the threat landscape or organisational context.**

Information Security Controls

ICDL implements a comprehensive set of information security controls, drawing from ISO 27001 Annex A and tailored to our organisation's specific requirements. These controls include:

- **Access Control**
- **Incident Management**
- **Business Continuity Planning**
- **Encryption and Cryptography**
- **Supplier Relationship Management**



Compliance and Auditing

ICDL conduct regular internal audits and reviews of the ISMS to ensure compliance with ISO 27001 requirements.

Additionally, external audits are conducted to validate our adherence to information security best practices and seek certification as evidence of our commitment to security excellence.

Incident Response

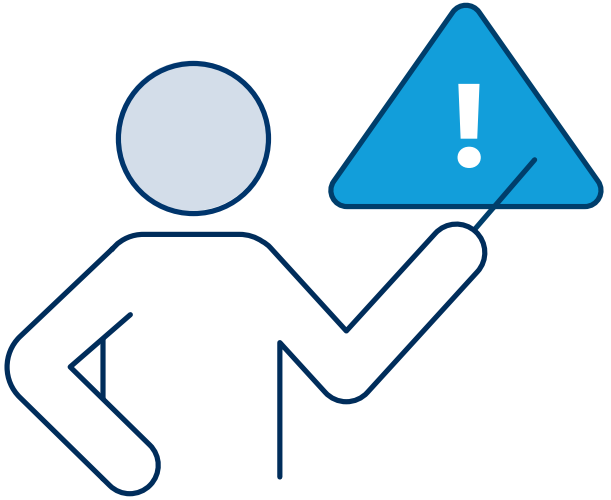
In the event of a security incident or breach, ICDL has established procedures for timely reporting, assessing impact, containing the incident, and initiating recovery efforts.

These procedures are designed to minimise disruption and mitigate the impact on our software platforms and certification services.

Security Awareness and Training

We provide comprehensive security awareness and training programs to all personnel to ensure they understand their roles and responsibilities in safeguarding information assets.

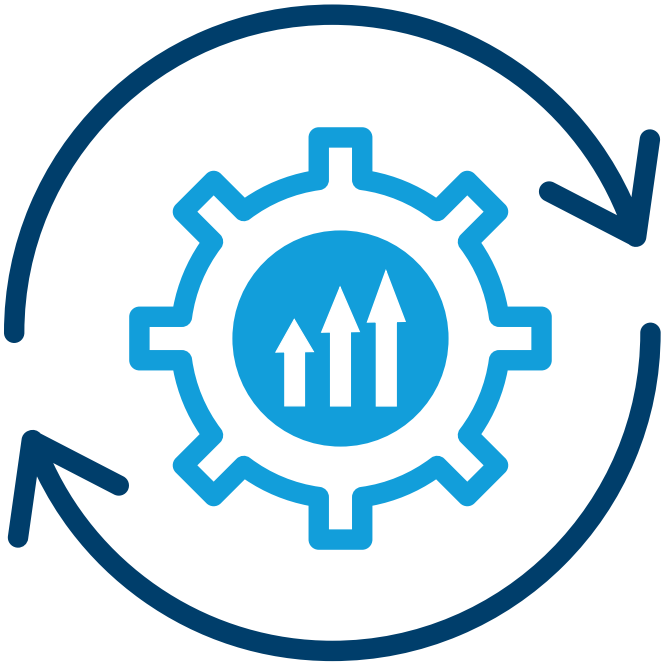
Regular updates and reminders reinforce the importance of information security best practices throughout the organisation.



Continuous Improvement

ICDL is dedicated to continuously improving the ISMS through ongoing monitoring, evaluation of security controls, and incorporation of lessons learned from security incidents or audits.

Feedback from stakeholders is encouraged to drive enhancements and ensure the effectiveness of our information security practices.



Conclusion

By adhering to this Information Security Policy, ICDL reaffirms its commitment to protecting the confidentiality, integrity, and availability of data within our software platforms and services. ICDL strive to maintain the trust of our stakeholders and uphold the standards of excellence in information security governance.

The Digital Skills Standard

Thank You

icdl.org/information-security-policy