Optimal Risk Training

Information Security Policy

Created by:	Compliance Lead
Document owner:	Managing Director
Approved by:	Center Manager
Confidentiality level:	Uncontrolled – may be disclosed externally, in full

Change history

Date	Version	Created by	Description of change
Jan 25	0.1	Compliance Lead	Rewrite and Renewal of ORT QMS

Table of contents

1. Scope

The policies apply to all staff involved in the delivery and administration of training services as well as any learners receiving training provided by Optimal Risk Training.

2. Target Audiences

Learners and or prospective learners so they be assured of our commitment to information security and the protection of confidential information.

Any individual who handles information on behalf of the Optimal Risk Training as part of their role (staff: including directors, sub-contractors, volunteers, and third parties carrying out an Optimal Risk Training function) must comply with this Policy.

3. Information security

Information security is achieved through an Information Security Framework of managed controls consisting of policy, physical restrictions, technical restrictions, user awareness raising, and organisational culture.

Information is essential for our day-to-day delivery of training services to our learners. We rely heavily on digital technology as well as minimal printed documents and other recorded information.

Failure to appropriately protect and secure this information may lead to serious data loss of Confidentiality, Availability or Integrity (CIA).

- Confidentiality – Allowing the information to be known to people that should not know
- Integrity – Allowing the data to be changed in a way it should not be changed
- Availability – Loosing access to the data when access is needed

Any loss of CIA may incur serious financial and reputational damage to the company.

We implement appropriate information security controls and practices to safeguard this information, while also enabling those that need to, to access and use the information they need.

This is supported by an ever-improving suite of policies and procedures, each authorised by the Managing Director to provide a robust Information Security Framework.

3.1. Policy Background and Foundations

This policy, is subordinate to the wider Optimal Risk Group Information Security Policy. Optimal Risk Training part of the Optimal Risk Group.

This Policy is based on the following standards, regulations, and legislation:

- ISO/IEC 27001 & 2
- NCSC Cyber Essentials Scheme
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

- ICO Guidance
- Investigatory Powers (Interception by Businesses etc, for Monitoring & Record Keeping Purposes) Regulations 2018 (normal course of business monitoring of communications)

4. Supporting topic specific Policies

An ever-improving suite of policies and procedures, each authorised by the Managing Director. These are published and available to appropriate staff members on a need to know, need to use and need to update basis. This includes, but is not limited to policies that deal specifically with:

- Data Protection Policy (policy relating to Personal Information – GDPR)
- User access control (policy controlling users access to our information)
- Administrator access control (policy controlling Administrator access to our systems)
- Acceptable use (policy detailing what is and not acceptable when accessing or using our information)
- Mobile Phone (or tablet) Policy
- Personal Device (BYOD) Policy
- Clear desk and clear working environment
- Objectives Policy
- Continual Improvement Plan

4.1.1. Users and Acceptable Use

Optimal Risk's Acceptable Use Policy (AUP) (see topic specific Policy) outlines expected behaviours that our users must comply with. The AUP includes rules for the acceptable and prohibited use of Optimal Risk's facilities and services, including responsibility for protecting Optimal Risk's information. It links to relevant misconduct and/or disciplinary policies in the event of misuse.

4.1.2. Training and Awareness

Optimal Risk is committed to supporting and promoting staff awareness of their information security responsibilities through a framework of policies, guidance, webpages, team briefings and staff mandatory e-learning courses.

Training is appropriate to role. Users with privileged or administrator access, or business areas who regularly handle high risk information, must undertake bespoke training, and adhere to documented operating procedures.

4.1.3. Objectives Policy

Information security objectives are those objectives established by Optimal Risk to help us improve our Information Security Management system, so that we may better prevent or minimise the impact of Information Security Incidents.

Optimal Risk operates a controlled system of setting and managing the achievement of information security objectives. See separate Objectives Policy.

4.1.4. Continual Improvement Plan

Continual Improvement of an Information Security Framework is essential to ensure the system keeps up with changes in technology, industry trends or lessons identified.

Optimal Risk Group operates a controlled system of Continual Improvement of our suite of policies and procedures, to maintain an ever-improving robust Information Security Framework. See Continual Improvement Plan.

5. Security by Design and by Default

Information security is most effective when using layers of security across physical barriers, organisational rules & procedures, technical barriers, and incident response / management. It is not sufficient to rely on outsourced IT Services, historical practices, or common sense.

When initiating new systems, or changing how information is used and processed, the security of the information must be of paramount importance, ahead of, but not hindering secure access by those that need it.

Each user is responsible for continually assessing security and requesting support or reporting concerns without delay.

6. Delegated accountability

Whilst the MD (Head Office) holds ultimate responsibility, accountability for the day-to-day operations must be delegated. Head Office will ensure centralised completed records are maintained, but department heads hold full accountability for activities within their departments.

Five simple principles apply:

- Understand what information we have and why that information is of use to us
- Understand what systems we use to store or access our information
- Maintain Asset Registers of equipment, information, user accounts and systems
- Understand and assess the risks, a loss of CIA of that information may introduce
- Capture and maintain that understanding in documented records

6.1. Understand what information we have and why that information is of use to us

This calls for clearly defined ownership of and responsibility for information used or generated.

6.1.1. Accountable Owners: Business / Data Owners

All information will have a clearly defined owner or custodian, this being the Business or Data Owner.

6.1.1.1. Business Owner

The Business Owner is usually the senior person responsible and accountable for the function that creates and uses that information from creation to consumption and end of use (e.g., Head Office, Finance, Head of Department, Consultant, Manager, etc.).

The Business Owner is responsible for any Data Owners within their department and ensuring that records are maintained and communicated with Head Office.

6.1.1.2. Data Owner

The Data Owner may be at any level in the organisation, with responsibility for protecting the information they have been entrusted with (e.g. an individual Operator, Investigator, Instructor, Consultant, Manager, etc.).

Data Owners are responsible for ensuring the data they handle is securely managed regardless of location i.e., whether in local systems, in Egnyte's cloud managed facilities and services or third party hosted solutions: each Data Owner is responsible for following any rules or processes around access, use, quality and accuracy, storage and security, and ensuring compliance with rules or processes.

6.2. Understand what systems we use to store or access our information

Systems are those software applications or cloud-based systems that we use to process our information. These include, but are not limited to:

- Egnyte – a cloud-based file storage system
- O635 – a cloud-based email and suite of office software tools
- Xero – a cloud-based accounting software tool

6.2.1. System Owners & Administrators

System Owners & Administrators are nominated roles: in charge of and responsible for managing the systems which we use to process our information.

System Owners & Administrators control user access and ensure each user may only access information on a need to know, need to use and or need to update basis.

System Owners & Administrators will only permit access to users when an application for access is approved by the relevant Business Owner.

6.3. Maintain Asset Registers of equipment, information, users accounts and systems

Business Owners & Data Owners must understand what data, infrastructure, IT equipment, information and IT systems, software, cloud services, and storage they use.

Business Owners & Data Owners (or their delegates), whether at a business area, temporary teaching facility, department, or any level must maintain and update an Asset Register (a list of what equipment and or information they use).

For IT devices, (computers, tablets, smart phones or cameras) it is critical for Head Office and Business Owners to be aware of new devices and systems before they are introduced into the organisation, to ensure end user devices are appropriately protected and managed.

Head Office maintain centralised asset registers, but this does not remove the accountability of Business Owners & Data Owners to maintain and control their own local records.

6.4. Understand and Assess the risks

When planning or developing new information systems, new Optimal Risk services, or new use of information, Business & Data Owners should give as much advance notice as possible to Head Office. This is to:

- ensure effective use of Optimal Risk resources (financial, infrastructure and workforce).
- prioritise workload against existing demands.
- ensure the system meets technical security baselines and design principles
- assess the impact, and integration with current Optimal Risk systems.
- assess and build in data protection privacy and transparency requirements.

This Information Security Policy supports Business & Data Owners and System Owners to work with Head Office to ensure risks are identified, recorded, assessed and if necessary treated.

Head Office will maintain centralised risk registers, but this does not remove the accountability of Business Owners & Data Owners to work with head office to identify and assess Information Security risks.

6.5. Capture our understanding in documented records

Head Office will maintain centralised records.

Head Office relies on Business Owners & Data Owners to ensure Head Office maintains awareness of activities at all levels.

Business Owners & Data Owners must maintain local records as evidence of compliance with this policy.

6.6. Incident Reporting:

All users of Optimal Risk Group information, IT facilities and services are responsible for reporting data loss and security incidents. Reports should be submitted without delay to Head Office and followed up by email to the compliance lead (see Suggestions, Complaints & Faults Reporting).

7. Business monitoring of communications

Any use or access to our systems is attributed to the individual user.

All uses of our systems are logged and may be monitored to ensure our information is being used as per our acceptable use policy.

In the event of a security incident, or disciplinary proceedings, records extracted from the normal course of business monitoring may be accessed by System Owners, Administrators or Head Office.

Users should expect that no access or use of Optimal Risk Group's systems is personal.

8. Policy Compliance

Failure to comply with this Policy and the Information Protection Guide in protecting Optimal Risk Group's information (or that entrusted to us by a third party) puts Optimal Risk Group at risk of reputational damage, financial penalty, breach of legal, contractual or regulatory requirement. It may

also lead to disciplinary action in accordance with the relevant Disciplinary Policy (employed staff) of Service Contract (contractors).