

QA 8.8 Data Protection Training and Awareness Policy

Contents

QA 8.8 Data Protection Training and Awareness Policy	1
1 QA 8.8 Data Protection Training and Awareness Policy	2
1.1 Policy Ownership	2
1.2 Purpose	2
1.3 Policy Scope	2
1.4 Policy Statement	2
2 Responsibilities	3
2.1 Responsibilities	3
3 Monitoring & Review	3
4 Version Control	4

1 QA 8.8 Data Protection Training and Awareness Policy

1.1 Policy Ownership

The policy owner is the Data Protection Manager

1.2 Purpose

This policy establishes a standard for educating and raising awareness among all employees, contractors, and third parties regarding data protection. It aims to foster a culture of security awareness, reduce the risk of human errors leading to security breaches, and ensure compliance with applicable laws, regulations, and organisational standards.

1.3 Policy Scope

This policy applies to all employees, contractors, and third parties who have access to the organisation's information systems, handle data, or are otherwise involved in activities that impact information security. It covers all training and awareness initiatives, including but not limited to onboarding training, role-based training, periodic refresher courses, and ongoing awareness programs.

1.4 Policy Statement

The organisation is committed to ensuring all personnel know and understand the importance of information security, data protection, and compliance. To achieve this, the organisation will implement a comprehensive Training and Awareness Program that includes the following components:

Induction Training:

All new employees, contractors, and relevant third parties must complete mandatory induction training on information security, data protection, and compliance within their first month of engagement.

Role-Based Training:

Tailored training will be provided based on specific roles and responsibilities, ensuring that personnel are equipped with the knowledge relevant to their functions, such as handling sensitive data, using specific IT systems, or managing compliance-related activities.

Ongoing Awareness Programs:

Regular security bulletins, newsletters, and email alerts will be distributed to inform all personnel about emerging threats, policy updates, and best practices.

Visual aids, such as posters and infographics, will be used throughout the workplace to reinforce security awareness.

Phishing Simulations and Security Drills:

Periodic phishing simulations and security incident drills will be conducted to assess employees' awareness levels and identify areas where additional training may be needed.

Refresher Training:

All employees and contractors must attend annual refresher training sessions to stay updated on the latest security practices, policies, and procedures.

Monitoring and Evaluation:

The effectiveness of the training and awareness program will be monitored through participation tracking, knowledge assessments, and regular audits.

Feedback will be collected from participants to improve the program continuously.

Compliance and Enforcement:

Participation in designated training programs is mandatory, and non-compliance may result in disciplinary action, including potential restrictions on system access or termination of employment or contract.

2 Responsibilities

2.1 Responsibilities

The following personnel are responsible for Data Management within Cenit College

Role	Responsibility
Policy Owner	- Develop and maintain the training and awareness program content. - Ensure the delivery of training sessions and awareness activities. - Monitor and evaluate the effectiveness of the training program. - Regularly review and update the policy to reflect new threats, technologies, and regulatory changes.
Human Resources (HR)	- Integrate security training into the employee onboarding process. - Maintain records of training completion and compliance. - Coordinate with the Data Protection Manager to schedule and communicate training sessions.
IT Department/ID Department	Provide technical support for delivering online training and managing e-learning platforms.
Employees, Contractors, and Third Parties	- Participate in all mandatory training and awareness sessions. - Apply the knowledge gained from training in daily tasks. - Report any security concerns or incidents to the appropriate authorities.

3 Monitoring & Review

The Board of Directors, in conjunction with the Data Protection Manager (DPM), will monitor this policy as part of the annual audit schedule to ensure its currency and appropriateness.

This policy will be reviewed annually or in response to significant organisational changes, legal requirements, or threat landscape. Any updates to the policy will be communicated to all relevant stakeholders. The organisation will regularly audit compliance with this policy and take corrective actions where necessary.

4 Version Control

Version	Date	Description	Originator	Approved by
1	21/11/2023	New QA System	Perri Williams	Board of Directors
2	23/06/2026	Policy renamed from QA 8.7 to QA 8.8 Placed into new Policy Template	Head of Quality	Board of Directors