

The Personal Learning Record for the Qualifications and Credit Framework Security Policy

Tier 2 Document
Version 1.0

April 2010

Of interest to everyone involved in learning and skills



MIAP
Managing Information
Across Partners

Contents

	Page
1 Purpose and Policy Overview	4
2 Policy Scope	4
3 Terminology	4
4 Compliance	5
4.1 Security Management Standards	5
4.2 Applicable Standards	5
4.3 Compliance with the Skills Funding Information Security Policy	5
4.4 Awarding Organisation Interface Specifications	5
5 Re-Approval Conditions	6
6 Security Forum	6
6.1 Scope	6
6.2 Purpose	6
6.3 Escalation	6
7 Abbreviations	6
8 Appendix 1 – ISO Security Policy Statements	7
8.1 Risk Assessment and Treatment	7
8.2 Security Policy	7
8.3 Organisation of Information Security	7
8.4 Asset Management	7
8.5 Human Resource Security	8
8.6 Physical & Environmental Security	8
8.7 Communications & Operations Management	9
8.8 Access Control	10
8.9 Information Systems Acquisition, Development & Maintenance	12
8.10 Information Security Incident Management	13
8.11 Business Continuity Management	13
8.12 Compliance	13

1. Purpose and Policy Overview

The Purpose of this Security Policy is to set out and explain to Awarding Organisations, the key security measures implemented by the Chief Executive of Skills Funding to protect the confidentiality, integrity and availability of the data.

This policy document is written by the Chief Executive of Skills Funding and is a Tier 2 Document as referenced by the Awarding Organisation Agreement for the Personal Learning Record (PLR) for the Qualifications and Credit Framework (QCF).

This document sets out the policy for the security of the information stored and processed by the system that provides the PLR for the QCF and the associated services which are developed and managed by the Chief Executive.

This policy captures the key data security principles in the safeguarding of Learner Achievement Data supplied by Awarding Organisations to the PLR for the QCF. It achieves this by proposing physical, procedural, personnel and technical countermeasures based on a risk assessment.

This document is intended to describe the security systems and processes to protect Achievement Data submitted by Awarding Organisations.

This document:

- is version controlled;
- identifies and correlates responsibilities to designated roles;
- states the security policies that must be adhered to in order to maintain the required level of security;
- defines the management and operation of systems and networks;
- defines the policies to be implemented by any subcontractors; and
- is intended to be read by the members of the Security Forum including representatives of the Awarding Organisation, Chief Executive and other interested parties who have a need to review and/or approve this document.

2. Policy Scope

This policy covers general IT security requirements, including information security, the logical elements, network security, environmental security, physical security, and the management of security relevant to the PLR for the QCF.

3. Terminology

The “**QCF System**” as used in this document means the software and hardware used to provide access to the PLR for the QCF.

The “**Service**” refers to the applications management, monitoring and support provided to enable the system to operate effectively.

4. Compliance

4.1 Security Management Standards

This Security Policy complies with the requirements of ISO27001: The International Standard for an Information Security Management System. This document is designed as a Summary of Controls (SoC) in accordance with the ISO Standard and it incorporates ISO Standard requirements.

The policy statements in this document represent the key countermeasures implemented to protect the confidentiality, availability and integrity of the data.

Some statements can be classified as meeting more than one of the ISO27001 controls. Where this is the case the primary control area has been used to categorise the statement. This has been modelled on the STREAM Risk Management Tool.

4.2 Applicable Standards

The following standards will be applied to the design, build and implementation of the System delivered through contractual arrangements with the suppliers to the Chief Executive:

- **HMG Security Policy Framework (SPF) v3.0** dated October 2009.
- **E-Government Interoperability Framework** (referred to as e-GIF) Version 6.1 dated 18 March 2005, available at <http://www.cabinetoffice.gov.uk/govtalk.aspx>, and its subsidiary Strategy Framework Policy and Guidelines.
- **The Official Secrets Act 1911 to 1989**
- **Data Protection Act 1988**
- **Freedom of Information Act 2000**
- **Privacy and Electronic Communications Act Regulations 2003**
- **ISO/IEC27001:2005** which is part of the security management plan of the suppliers to the Chief Executive.

4.3 Compliance with the Skills Funding Information Security Policy

The Skills Funding Information Security Policy has been reviewed for the purposes of writing of this document and the Chief Executive may review this Policy as necessary.

4.4 Awarding Organisation Interface Specifications

Information relating to the secure transfer of Learner Achievement Data from Awarding Organisations to the PLR for the QCF will be defined in more detail in the relevant Awarding Organisation interface specifications.

This information will address the different file transfer methods (web services, xml etc) and the relevant supporting security measures such as but not limited to encryption levels, file headers and validation checks.

It is expected that this agreement will be updated to reflect the data interface security measures following the release of the interface specifications.

5 Re-Approval Conditions

This Security policy will need to be re-approved:

- prior to any new network connections being installed;
- if there is a change in the way in which the QCF System is used or operated (e.g. by the addition of a new application); and
- if the risk assessment indicates that there is significant change or agreed contractual change which warrants a document review.

6 Security Forum

6.1 Scope

The scope of the Security Forum will be limited to the Terms of Reference as set out in Schedule 2 of the Awarding Organisation Agreement.

6.2 Purpose

The purpose of this group is to improve user input into the management of security, provide a basis for critical incident response management, and advise the senior information risk owner for the service. This Security Forum will therefore have responsibility for providing advice on:

- Security procedures;
- Incident management processes; and
- Threats.

The Security Forum will also advise the senior information risk owner on impacts of changes to the Service Charter, including a review of the risk management accreditation document set, and inform the Customer Scrutiny Group.

The Security Forum will be responsible on behalf of the sector for reviewing the operation of the PLR against the security policy.

In the event of a critical incident, members of the Security Forum may be requested to become part of an incident response team should this be necessary.

6.3 Escalation

The Security Forum may escalate issues to the senior information risk owner for Skills Funding as well as the Head of MIAP Service and to the Customer Scrutiny Group.

7. Abbreviations

AMC	Application Management Centre
CRAMM	Originally the CCTA Risk Analysis and Management Method.
DRSE	Disaster Recovery and Staging Environment at Docklands
ISMS	Information Security Management System
QCFSM	QCF Security Manager
PE	Production Environment
SDM	Service Delivery Manager
SLA	Service Level Agreement
SoC	Summary of Controls
SYOPs	Security Operating Procedures

8. Appendix 1 – ISO Security Policy Statements

Introduction

The following policy statements are those deemed to be relevant to the PLR for the QCF and its environment. These policy statements highlight the key security measures implemented by the Chief Executive to ensure the confidentiality, integrity and availability of the data in the PLR for the QCF system. They are arranged in sub-groups which map onto the eleven areas of ISO27001 controls.

In some cases it has been considered appropriate to highlight individual countermeasures hence some statements have duplicate references.

Where the Contracts require specific measures to be taken these have been highlighted.

8.1 Risk Assessment and Treatment

Risk Analysis shall be undertaken to assess the need for implementation of additional security measures, and expenditure on security measures shall always be justified on the basis of risk analysis.

8.2 Security Policy

There shall be management direction and support for information security.

8.3 Organisation of Information Security

8.3.1 Internal Organisation

- A management framework shall be established to initiate and control the implementation of Information Security.
- The security requirements and available security measures for Network Services provided by third parties shall be formally agreed and documented.
- Out-source and facilities management companies and suppliers need a clear statement of the business requirements for system access included in their contracts.

8.4 Asset Management

8.4.1 Responsibility for assets

- Documents and records whether held on paper or electronically shall be produced in an approved manner and be appropriately identified and protected.
- All information and data shall be labelled according to its level of sensitivity as defined by the Chief Executive's Data Classification and Labelling Policy (DCLP) and handled in accordance with HMG Guidance on handling information marked 'PROTECT'.
- Information being exchanged over the phone shall be protected.

8.4.2 Information classification

- The security classification of information shall be exported with the information in order that the receiving system can impose an equivalent level of access control.
- Care shall be taken when exporting information to another organisation to ensure that the receiving organisation will provide the necessary level of protection to the information:
 - Printed information shall be labelled with its classification so users can identify how the documents need to be handled; and
 - Documents shall be destroyed according to their classification.

8.5 Human Resource Security

8.5.1 Prior to Employment

- Job descriptions shall be clearly defined;
- All permanent, contract, and temporary staff shall undergo pre-employment screening and together with suppliers to the Chief Executive, shall not be allowed access to live QCF and PLR data unless they have undergone standard CRB security checks; and
- All permanent, contract, and temporary staff shall sign a confidentiality agreement.

8.5.2 During Employment

- Staff shall receive training, direction and supervision in their work. Staff shall be kept aware of security issues through education and training.
- Staff shall be given clear instructions on actions to be taken relating to bomb threats:
 - safety of personnel in the event of fire shall be addressed; and
 - disciplinary procedures shall be in place to deal with security breaches.

8.5.3 Termination or Change of Employment

All employee access rights and identification badges shall be removed on leaving Skills Funding.

8.6 Physical & Environmental Security

8.6.1 Secure Areas

- Guards shall be employed as a deterrent to criminals.
- The Chief Executive in providing the PLR for the QCF shall be prepared for a receipt of potential letter bombs or threat warnings:
 - site surveys to identify vulnerabilities shall be carried out;
 - fire prevention measures shall be in place; and
 - fire detection measures shall be implemented. Measures for controlling fires shall be in place. Access by maintenance staff and/or visitors shall be controlled. Measures to prevent theft of property from offices, rooms and facilities shall be implemented.

8.6.2 Equipment Security

- IT equipment shall be maintained in an appropriate environment.
- Distribution and network termination equipment shall be physically protected.
- The physical security of equipment used to process, store or transmit information shall be maintained.
- Measures to prevent the theft of computer equipment shall be implemented
- Measures to control the flow of water in a leakage shall be implemented.
- Measures to detect and prevent water penetration or damage shall be implemented. Measures shall be in place to protect against a natural disaster.
- Working environments and equipment rooms shall have a resilient conditioned power supply.
- Power equipment shall be installed according to relevant regulations.
- Network cables shall be physically secured against wire tapping. Equipment shall be appropriately maintained. All key equipment shall be supported by an appropriate programme of maintenance.

8.7 Communications & Operations Management

8.7.1 Operational Procedures & Responsibilities

- There shall be formal documented procedures to cover all operator actions.
- Access to System Administrator IDs shall be tightly controlled. The identity of software maintenance engineers shall be checked to reduce the risk of unauthorised people gaining access to the information.

8.7.2 Third Party Service Delivery Management

This is covered under policy statements in Paragraph 8.3.1.

8.7.3 System Planning & Acceptance

Acceptance criteria shall be established against which suitable tests shall be carried out prior to acceptance of a system as providing the required level of security.

8.7.4 Protection Against Malicious and Mobile Code

- Procedures to minimise the potential for the introduction of malicious software shall be implemented.
- Any identified malicious software shall be isolated and removed.

8.7.5 Back-up

Data Back-ups shall be taken.

8.7.6 Network Security Management

- Network management shall be undertaken in a secure manner and provide support for the management of network security
- Network monitoring shall be implemented to allow early detection of unauthorised use, detection or failure.

8.7.7 Media Handling

- Procedures shall be implemented to ensure that deletion of any data or sensitive software is such that it cannot be recovered.
- Media shall be labelled in order to ensure correct handling.

8.7.8 Exchange of Information

Security of media shall be maintained in transit.

8.7.9 Electronic Commerce Services

- External e-mail and e-commerce services shall be available for use when required and shall only be used for approved business activities.
- Interfaces between outward facing e-commerce systems and internal systems and networks shall be clearly defined and controlled.

8.7.10 Monitoring

- Audit Logs shall have sufficient capacity.
- Sufficient information shall be recorded to enable a thorough review of any suspected incident to be completed.
- Auditing is concerned solely with the analysis of security relevant events that take place on a system.
- Audit trails shall be reviewed to ensure that users are only performing processes that they have been explicitly authorised to carry out.
- Trusted Facilities Management shall be used to ensure that all events that the System Administrator has specified to be included in the ID Log, where available, will be written to the Log, and that no unauthorised modification of the Log can be made.
- The time events occur may be significant in investigating any security incident. It is therefore important that all clocks of connected systems are working to a common standard.

8.8 Access Control

8.8.1 Business Requirement for Access Control

- All users of the system shall be identified and authenticated by allocation of a unique username and password.
- All systems interacting with the PLR for the QCF shall be authenticated and comply with this policy.
- Laptops and other mobile media storage devices use to store and/or process 'PROTECT' data shall be encrypted.
- Possession and issue of system access rights shall be under the control of system management (e-GIF).
- Access to privileged functions shall be restricted to those people who have a need to use them.

8.8.2 User Access Management

- Passwords shall be generated in a manner that makes them difficult for an unauthorised person to guess.
- Passwords shall be sufficiently long so that they are difficult to guess or determine from the encrypted form.
- Passwords shall be distributed to users in such a manner that the confidentiality of the password is maintained.
- Dual factor authentication, such as tokens, shall be used to provide greater confidence in the identification of a user where access to the data within the full PLR for the QCF is required.
- User's access rights shall be reviewed in order to maintain effective control over access to data and IT services.
- Passwords shall be changed frequently to assist in ensuring that the confidentiality of the password continues to be maintained.
- It shall be possible to revoke user access rights.

8.8.3 User Responsibilities

- The security of information in printed documents shall be maintained whilst in storage.

8.8.4 Network Access Control

- Modem access to systems shall be controlled.
- All remote diagnostic ports shall be protected from unauthorised access.
- User access shall be segregated across networks, especially when connected to third party networks.
- Connection with the Internet to be secured.

8.8.5 Operating System Access Control

- Passwords shall be stored in a form that no one, not even the System Administrator, may see the password chosen by the user.
- The log-on authentication dialogue shall not assist unauthorised users in any attempt to gain unauthorised access.

8.8.6 Application and Information Access Control

- The time that a workstation can remain inactive, while logged on, shall be minimised to reduce the opportunity for an unauthorised person to impersonate a legitimate user.
- Access to system data shall be specified by the Data Owner and limited to those users with permission to access it.

8.8.7 Mobile Computing and Teleworking

Out of office working shall be secured.

8.9 Information Systems Acquisition, Development & Maintenance

8.9.1 Security Requirements of Information Systems

- Security requirements of applications shall be specified.
- Ensure that the necessary authorisation is obtained throughout the process in order to control the development of applications (including use of office products such as Excel and Access).

8.9.2 Correct Processing in Applications

- The application shall ensure that all data input (whether through a batch load or by user keying) is fully validated and rejected if unsuitable.
- Validation rules shall be applied to prevent personal sensitive data (as defined by the Data Protection Act) from being entered.

8.9.3 Cryptographic Controls

- The confidentiality of information in transit over networks shall be protected.
- Public Key and digital signature based protection shall be used to protect confidentiality, integrity, authenticity and non-repudiation of transactions.

8.9.4 Security of System Files

- The integrity of software shall be maintained in live use.
- The integrity of application systems, data and PCs shall be maintained.

8.9.5 Security in Development & Support Processes

- Changes to the application shall be regulated in order to control the development of applications.
- All changes to software shall be authorised before they are implemented. Changes to software, which have to be made before the authorisation can be granted, shall be controlled and kept to a minimum.
- Periodically, it is necessary to change the Operating System (e.g., when installing a new version). When such changes occur, the security of the system shall be reviewed to ensure that it has not introduced any adverse affects.
- The development of applications shall be controlled by following development standards to ensure vulnerabilities are not introduced.
- Access to System Administration utilities shall be accounted for.
- When software is being maintained there is a risk that errors may be made which could lead to loss of availability, disclosure or modification of information, so such work shall be checked.

8.9.6 Technical Vulnerability Management

- Independent Tests to include Pen Testing shall be conducted prior to acceptance of a system as providing the required level of security.
- Tests shall be conducted prior to acceptance of the configured Web server to ensure it provides the required level of security.

8.10 Information Security Incident Management

8.10.1 Reporting Information Security Events and Weaknesses

Security incidents shall be detected, reported to enable analysis, any damage managed and lessons learnt disseminated.

8.10.2 Management of Information Security Incidents & Improvements

- Security incidents shall be managed in a consistent and effective manner.
- When incidents are detected or suspected they shall be investigated in a thorough manner which cannot be compromised.
- Potential system abuse must be investigated in a forensically sound manner and in line with current legal guidelines.
- The workstation identifier shall be used to assist in investigation of any specific security-related incidents.
- The Audit Log shall be retained for a period commensurate with the business requirements.

8.11 Business Continuity Management

8.11.1 Information Security Aspects of Business Continuity Management

- Business Continuity Plans shall be prepared.
- Backup or stand-by hosts shall be available when required.

8.12 Compliance

8.12.1 Compliance with Legal Requirements

Organisations such as the suppliers to the Chief Executive and System Users shall comply with Data Protection and Computer Misuse legislation (where it applies) and other requirements as required by law.

8.12.2 Compliance with Security Policies and Standards and Technical Compliance

The PLR for the QCF shall be compliant with Skills Funding's Information Security Policy, e-GIF standards and follow CESG guidance where appropriate.

8.12.3 Information Systems Audit Considerations

This is covered by sub-section 8.7.10.

Skills Funding Agency Office
Contact details for each office can be
found on our website:
www.skillsfundingagency.bis.gov.uk

Skills Funding Agency

National Office

Cheylesmore House
Quinton Road
Coventry CV1 2WT
T 0845 377 5000
F 024 7682 3675

www.bis.gov.uk/skillsfundingagency



© Skills Funding Agency

Published by the Skills Funding Agency

Extracts from this publication may be reproduced for non-commercial, educational or training purposes on condition that the source is acknowledged and the findings are not misrepresented.

This publication is available in electronic form on the Skills Funding Agency website:

www.skillsfundingagency.bis.gov.uk

If you require this publication in an alternative format or language, please contact the Skills Funding Agency Help Desk: 0870 900 6800.

Skills Funding Agency – P – 100005