Cabot
Learning
Federation

CLF Information Security Policy

Author:

Andrew Ling | Head of ICT Services

Date of issue:

16/09/2015

Record of Issue

Date	Page	Change	Origin of Change
Date	Pages / Whole document	Description of Change	Origin of change (e.g. routine update, request for review)
29/05/2015	Whole document	Document framework created	
09/06/2015	Whole document	Completed required sections from ISO standards following benchmarking of external sources	
13/07/2015	Whole document	First draft complete	
16/09/2015	Whole document	Final version pending Board approval	

Distribution

Organisation	Contact	Copies
Organisation	Name	e.g. electronic
CLF	CLF Board	Paper

Cabot Learning Federation

Contents

1 Information Security Organization

1.1 Information Security Policy

This policy is based on standards and definitions from the ISO27001 and the GOV.UK service manual for Information Security.

The policy is divided into a number of sections as defined by ISO27001 and supported by security measures in use throughout the CLF as well as industry recognised mechanisms.

There are a number of supporting policy documents that are referenced throughout, which include:

- Flexible Working policy;
- Data protection policy
- Freedom of Information policy;
- Password and Encryption policy;
- Data retention policy.

1.1.1 Information Security policy

Information can be stored on computers, transmitted across networks, held on paper, held on digital removable media and transmitted in conversations. All forms of information must be protected.

The growth of distributed network and cloud systems presents opportunities for unauthorised access to computer systems. As personal mobile devices become more prolific, access to systems can take place on many devices outside the management scope of CLF ICT systems. As such there is a greater need for departments and all employees to take sufficient responsibility for information security.

Information security refers to the theory and practice of defending data or information systems against:

- Unauthorised or unintended access
- Destruction
- Disruption
- Tampering

There are 3 main concepts that support the management of information security. These consist of:

- Confidentiality - the assurance that information is not disclosed to individuals or systems that are not authorised to receive it;
- Integrity - the assurance that information can't be modified by those who are not authorised to modify it, or that any such modifications will not pass undetected;

- Availability - the assurance that information is available when it is needed, and that mishap or malice cannot affect the ability of systems to provide information when requested.

The CLF will use a number of controls to support the management of information security which include:

- Physical - walls, locked doors;
- Procedural - training, processes;
- Regulatory - policies, rules of conduct;
- Technical - cryptographic software, use of secure protocols.

The Information Security policy ensures business continuity and minimises business damage by preventing and diminishing the impact of security incidents. The policy enables information to be shared, but ensures the protection of that information and related ICT assets.

Some controls are not applicable to every ICT environment and should be used as appropriate. However decisions about non-application must be made and documented by the HoIS.

1.1.2 Senior Management Support

The CEO and CLF Leadership Team are committed to ensuring that the effective information security controls are in place across the CLF.

The implementation of information security must be supported by all CLF SLT teams, and adhered to by all CLF staff.

The CLF will nominate a Head of Information Security (HoIS) who is responsible for the identifying and mitigating security risks to the CLF as a whole. However other staff also have important responsibilities within this policy and all staff are required to understand their role in compliance with this policy.

1.1.3 Information Security Policy Review

The Information Security Policy is reviewed on an annual basis through the Information Security Group (ISG).

2 Classifying Information And Data

2.1 Setting Classification Standards

2.1.1 Defining Information

This document makes reference to information security owners (ISO), and information security managers (ISM). These roles and definition are described as follows:

Role	Details	Responsibilities	Example
ISM	Owns the infrastructure of the system.	Updates to system; security of system; following processes for managing access and enabling access;	SIMS manager Active directory manager.
ISO	Owns the information	Grants access to information; Reviews access to information; Keeps data up-to-date;	SIMS manager Active directory manager. Department manager of a secured folder. Library system manager.

All ICT equipment owned or operated by CLF are considered hardware assets of the CLF.

All software owned or licensed by CLF are software assets of the CLF.

The contents of all digital forms of information, including but not limited to databases, mailboxes, word processed documents, spreadsheets, web pages, data files or configuration files, created by staff, students, Academy Councillors, Board members or third parties in the course of their duties are information assets of the CLF.

All such assets are collectively referred to as ICT Assets and must be accounted for and have a nominated owner.

An inventory of hardware software and information assets will be maintained, clearly identifying an owner and purpose.

It is the responsibility of the HoIS to ensure the inventory is regularly reviewed. It is the responsibility of the nominated owner of an asset to ensure any changes to configuration, usage or location are approved and reflected in the inventory.

It is the responsibility of each asset owner to ensure that access to the assets for which they are responsible is controlled and managed in accordance with the Information Security policy.

2.1.2 Classifying Information

The CLF has adopted four key definitions that underpin the principals of information security. These classification levels explicitly incorporate the Data Protection Act's definitions of Personal Data and Sensitive Personal Data, defined in detail in the CLF's Data Protection Policy.

1. Confidential

'Confidential' information is of significant value to CLF. Unauthorized disclosure or dissemination could result in severe financial or reputational damage to CLF, including fines of up to £500,000 from the Information Commissioner's Office.

Data that is defined by the Data Protection Act as Sensitive Personal Data falls into this category. Only those who explicitly need access must be granted it, and only to the least degree in order to do their work (the 'need to know' and 'least privilege' principles). When held outside CLF, on mobile

devices such as laptops, tablets or phones, or in transit, 'Confidential' information must be protected behind appropriate encryption at the device, drive or file level.

2. Restricted

'Restricted' information is subject to controls on access, such as only allowing valid logons from a small group of staff. 'Restricted' information must be held in such a manner that prevents unauthorised access i.e. on a system that requires a valid and appropriate user to log in before access is granted. Information defined as Personal Data by the Data Protection Act falls into this category. Disclosure or dissemination of this information is not intended, and may incur some negative publicity, but is unlikely to cause severe financial or reputational damage to CLF. Note that under the Data Protection Act large datasets of 'Restricted' information may become classified as Confidential, thereby requiring a higher level of access control.

3. Internal Use

'Internal use' information can be disclosed or disseminated by its owner to appropriate members of CLF staff and other individuals, as appropriate by information owners without any restrictions on content or time of publication.

4. Public

'Public' information can be disclosed or disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

Throughout this policy references to 'Critical' information include any information that can be defined as either confidential or restricted.

All Management Information Systems (MIS) contain sensitive-personal data and as such should be treated as confidential.

2.1.3 Labelling Classified Information

Any emails containing confidential information, encrypted or otherwise should be labelled as confidential in the subject.

Documents that are shared or presented and contain confidential information must be labelled as confidential in the title.

3 Controlling Access To Information And Systems

3.1 Controlling Access to Information and Systems

CLF will provide all staff, students, Academy Councillors, Board members and third parties with access to information they need to carry out their responsibilities accordingly.

3.1.1 Managing Access Control Standards

Access to information is appropriately controlled according to the information classification and the methods by which are deemed acceptable for access.

Access control standards will include explicit logon to devices, Microsoft Windows shares and file permissions; user access privileges; server and workstation access rights; firewall permissions; Microsoft Active Directory group membership; database access rights; Wi-Fi authentication; encryption and other mechanisms as required.

3.1.2 Managing User Access

Access to CLF systems will be provided through a unique user ID and complex password.

Staff user accounts must be requested and processed through the ICT service by department managers, with the appropriate ISO granting access as appropriate.

Remote access to systems from outside the CLF network will be explicitly permitted though the ICT service by department managers with the appropriate ISO granting access as appropriate.

Access to Restricted or Confidential areas will be explicitly permitted only by ISO.

On termination of contract staff accounts will be disabled but remain complete for a minimum of 30 days. The user account will then be subject to the ICT staff leaver process. Disabled and de-activated users may only be reactivated on verification of the respective user.

Generic or group user accounts must only be granted if sufficient controls are in place to secure information.

3.1.3 Securing Unattended Devices

Any devices which provide access to Internal Use, Restricted or Confidential information must be secured appropriately when not attended. This might be achieved through, but not limited to locking a workstation computer, or ensuring a suitable PIN number is applied to a mobile phone.

3.1.4 Management Duties

The allocation of super-user permissions such as local administrators, domain administrators, and system managers must be restricted and only permitted where necessary.

Super-user accounts must be assigned to individuals only, and not shared. Use of generic administrator logins on server systems is not permitted.

3.1.5 Third Party Service Management

Third parties are provided with accounts that permit them access to systems and information accordingly.

At the end of the contract period accounts will be managed as defined for staff accounts

Unless operationally necessary, and as recorded in the information owner schedule, third party accounts will be disabled when not in use.

3.1.6 Managing Network Access Controls

Reasonable measures must be taken by all ISM to ensure that information system are secured at the network layer, through the use of firewall systems and appropriate network segregation.

3.1.7 Controlling Access to Operating System Software

Where required on user assigned devices, users may be delegated local administrative permissions.

3.1.8 Managing Passwords

All passwords must be issued and subsequently managed through strict control and formal process, as defined in the CLF Password policy.

Passwords complexity for critical information systems are defined in the CLF Password policy and must be changed in accordance with this standard.

3.1.9 Securing Against Unauthorized Physical Access

Designated server equipment used to host information systems must be secured such that only authorised personnel are able to enter.

3.1.10 Access Policy

Access to critical information assets will be controlled by the ISM and granted by ISO who have ensured there is an appropriate business need for that access. Controls for access will include:

- Registering authorised users and defining access permissions;
- Ensuring users are aware of their responsibilities for information security;
- Ensuring suitable network access control is part of the network operating systems;
- Restricting access to critical information;
- Monitoring usage of specific resources as appropriate;
- Reviewing users and user access permissions regularly.

3.1.11 Monitoring System Access and Use

Systems must provide information on usage, including but not necessarily limited to logs of successful and failed login attempts. These should be reviewed regularly.

3.1.12 Controlling Remote User Access

Where remote access to critical information is permitted, the ISM must ensure that appropriate security measures are in place to protect the data from unauthorised access.

Remote access must be explicitly controlled and auditable, using specific group membership for the control rather than generic groups.

4 Processing Information And Documents

4.1 System Operations and Administration

Operating procedures and detailed instructions must be in place for all operational information systems, to ensure their correct and secure operation. Documented procedures are also required for

any systems development, maintenance and testing, especially where it involves cross-functional activities with other groups.

As a minimum, system documentation should include the following:

•Initial setup or configuration information;

•Inter dependencies with other parts of the ICT infrastructure;

•Support contacts;

•Back up and system recovery procedures;

•Relevant operating procedures;

•Username information and credentials stored in secure locations or in escrow.

4.1.1 Appointing System Administrators

Users that are permitted super-user access to information systems must be fit and capable of managing and maintaining that system. Where a user is unable to comply with this clause the ISM must be informed and take relevant action.

4.1.2 Administrating Systems

Users must only administer systems they have been granted access to and may only administer such systems where they are fit, able and appropriately trained.

Users should not assume authorisation to administer based on user privilege alone. When in any doubt the ISM must be informed and support requested if required.

4.1.3 Controlling Data Distribution

Critical information must remain in known, compliant locations at all times. Where information is moved between locations for operational or maintenance purposes any transient locations must provide the minimum level of protection required.

4.1.4 System Utilities

To reduce the risk of malicious software, only well known, standard system utilities should be used for maintaining information systems.

4.1.5 Managing Electronic Keys

All keys used for securing information or licensing software must be logged within the inventory. The specific security keys or certificates should then be stored within an identified secure location.

This includes but is not limited to security certificates used on websites and license keys for software.

The inventory information should indicate any expiry dates, to facilitate the proactive maintenance and renewal of services as required.

4.1.6 E-mail and Internet

Use of email and internet is restricted and appropriate use is defined the CLF Internet and Email Acceptable Use Policy.

4.1.7 Telephone & Fax

Use of telephony and fax is restricted and appropriate use is defined in the Email and Internet Acceptable Use Policy.

4.1.8 Information Retention Policy

The ISO must ensure that data within information systems is kept up to date and retained in accordance with the CLF Data Retention Policy.

4.2 Backup, Recovery and Archiving

The ISMs must ensure there is an appropriate disaster recovery process in place to protect all information systems.

These systems must be documented, tested and reviewed regularly.

4.2.1 Sharing Information

When any user sends information to any other user, internally to CLF or otherwise, steps must be taken to ensure that the information is appropriately secured during transit and that critical information will not subsequently reside in a location that would put the information at risk.

The sharing of critical information is not recommended by email, unless the recipient is within the organisation or the information is encrypted to a level as defined in the CLF Password policy.

Where the recipient is outside of CLF the recipient address must be validated as correct.

4.2.2 Protecting Documents with Passwords

Protecting documents with passwords is considered a reasonable method for securing restricted or confidential information in transit, provided the password and encryption methods are in compliance with the CLF Password policy.

In instances where encrypted files are shared the password or key must be sent via an alternate transport to the file itself.

A user may be required to unlock a password protected file if required by the ISO or HoIS.

5 Purchasing And Maintaining Commercial Software

The procurement of new information systems must be subject to a review to determine all information assets are secured appropriately.

Updates, configuration changes and operational maintenance should be undertaken in a controlled manner. The ISMs must ensure appropriate testing, backups and roll-back capabilities are implemented as appropriate.

5.1 Purchasing and Installing Software

All software and information systems purchased must be logged in the inventory, ensuring that relevant ownership, purpose and expiry information is captured.

It is the responsibility of the identified owner of the software to ensure that any license is renewed with the support of the ICT service if required.

5.1.1 Using Licensed Software

All licensed software should be inventoried and reviewed regularly.

Where a software license has expired the ISOs must ensure any related software is uninstalled in line with the license agreement, or renew the agreement.

6 Securing Hardware, Peripherals And Other Equipment

6.1 Using Secure Storage

ICT facilities supporting critical business activities must be housed in secure areas protected from unauthorised access, damage and interference. They must be protected by a defined security perimeter, with appropriate entry controls and security barriers and any specific environmental conditions recommended by the manufacturer or supplier.

Where this provision is not available an action plan will be drawn up and implemented to reduce the risk.

Digital removable media such as USB sticks should not be regularly used as a means for storing information, due to their reduced reliability and vulnerability to loss. In cases where digital removable media are required critical information must only be stored on devices that are encrypted to a level as defined in the CLF Password policy.

6.1.1 Taking Equipment off the Premises

Any devices that are to be used outside of CLF premises and contain critical information must be protected from unauthorised access. In the case of mobile laptop devices these must be encrypted to a level as defined in the CLF Password policy.

In the event that a mobile device containing critical information is lost or stolen, the ISM for that information must be informed immediately.

Special care must be taken to protect mobile devices (laptops, mobile phones, USB keys, PDAs etc.), due to the relative ease with which these may be stolen. Users of such devices will observe the following rules:

- Never leave them unattended in a public place;
- Do not loan mobile devices to friends or family members;
- Never leave equipment in a parked car or near a window;
- Take reasonable steps to secure equipment away at night if left in the office or home.

7 Combating Cyber Crime

7.1.1 Installing Virus Scanning Software

All networks systems, servers and managed devices should have anti-virus software installed to reduce the risk of malware infection.

Anti-virus systems servers should be configured to received definition updates on an hourly basis.

These systems should be regularly monitored.

8 Dealing With Premises Related Considerations

NOT CURRENTLY IN USE

9 Delivering Training And Staff Awareness

9.1 Awareness

The following controls will support an awareness and appropriate management of information security by all staff:

- All CLF staff will be made aware of the importance of information security and their responsibility for maintaining this;
- ISO must ensure staff granted access to critical information systems understand their duties and responsibilities in keeping the information secure;
- Any breaches of information security must be reported to the HoIS;
- Any staff that identifies a present or potential threat to information security should inform the ISM or HoIS;
- If a training need is identified the appropriate training will be provided to staff. Completion of such training will be documented.

10 Complying With Legal And Policy Requirement

ISO must hold regular reviews of the compliance of their systems in order to meet the CLF's Information Security policy, standards and other legislative and non-legislative security requirements.

11 Detecting And Responding To Information Security Incidents

11.1 Reporting Information Security Incidents

If a breach of information security has been identified the HoIS must be informed, who will then investigate and take action accordingly.

12 Planning For Business Continuity

NOT CURRENTLY IN USE