LSIILARE9v2

Manage content and collections for business continuity and information security

Overview

Organisations require systems to counteract and prevent interruptions to their activities and to protect critical processes from the effects of major failures or disasters. This standard is about developing and implementing policies for managing information assets and vital records, including safeguarding sensitive information and records, such as corporate information and customer information. It includes the enabling of secure information sharing.

This standard is applicable to people in management, practitioner and operational roles with responsibilities for information assets and vital records, and for implementing agreed security policies and strategies. It is also relevant for people with responsibility for ensuring authorised access to and use of information assets.

Performance criteria

You must be able to:

P1 provide management direction and support for information security, demonstrate that information security is being taken seriously and that effective steps are in place

P2 promote a strategic approach to securing the organisation's knowledge and information assets and collections

P3 identify vital records and other information assets critical to your organisation's business and the level of protection required

P4 ensure that proper attention is given to information assets and vital records in your organisation's business continuity planning

P5 ensure that your area of responsibility manages information assets and vital records in accordance with business continuity policies

P6 identify developments in information assets and vital records that require current business continuity plans to be amended

P7 develop and apply processes for establishing customer's identity, their eligibility to use/access information and collections and to enable secure access to information and collections

P8 identify, quantify, and manage the range of threats to electronic information in the organisation

P9 develop and implement policies and procedures that reduce the risks to physical records and collections of human error, theft, fraud or misuse of facilities

P10 monitor the application of information security processes by the organisation or ensure that monitoring is undertaken by the appropriate function

P11 develop contingency plans and procedures for disaster recovery and for salvage of materials, both physical and electronic

Knowledge and understanding

You need to know and understand:

K1 the importance of information security to your organisation and to your customers

K2 your organisation's business continuity plan

K3 current practices and issues in business continuity

K4 the implications for information, records and archive management of relevant national and international standards and guides to good practice, e.g. BS 25999 and the Business Continuity Institute standards

K5 how to influence stakeholders to feature information assets and vital records in business continuity plans

K6 the information content, collections and records acquired and created by the organisation and their implications in terms of information risk and security

K7 how the organisation uses key information, collections and records

K8 the information sharing security standards (ISS) employed by the organisation

K9 your and others' responsibilities for information security

K10 the range of standards and guides to good practice developed by national and international organisations, e.g. BSI/ISO and the Information Security Forum

K11 asset protection, recovery and disaster planning techniques and facilities

K12 the impact of any changes in ISS controls on customers and others

Additional Information

Behaviours

1. You judge what content, collections and assets have implications for business continuity and work closely with those in your organisation with responsibility for business continuity management
2. You champion the need to include information and vital records in business continuity plans
3. You recognise the impact that information security controls have on customers
4. You work to reduce risk, and promote compliance with standards and processes for information security to colleagues and customers.
5. You comply with business continuity policies and practices in your own work
6. You are sensitive to breaches of security and their importance

Links to other NOS

This standard links with the NOS for Health Informatics, developed by Skills for Health. See www.skillsforhealth.org.uk

The Skills Framework for the Information Age (SFIA) provides a common reference model for the identification of the skills needed to develop effective information systems (IS) and includes a number of standards relevant to this area. See www.sfia.org

The Business Continuity Institute has developed 10 standards of professional competence which provide an overview of good business continuity practice and relate to this standard. See www.thebci.org/10Standards.pdf

LSIILARE9v2

Manage content and collections for business continuity and information security

Developed by	Learning and Skills Improvement Service
Version number	1
Date approved	April 2008
Indicative review date	April 2010
Validity	Current
Status	Original
Originating organisation	Lifelong Learning UK
Original URN	LAISE9
Relevant occupations	Information and Communication Technology; Arts, Media and Publishing; Public Services; Professional Occupations; Information and Communication Technology; Research Professionals; Librarians and Related Professionals; Local Area Archives; Microfilm and Microfiche Technician; Publishing and information services; Language, literature and culture; Education and training; Teaching and lecturing; Direct learning support; Teaching Professionals; Public Service Professionals; Government and Related Organisations; Records; Communications; General; Public Service and Other Associate Professionals
Suite	Information and Library Services, Archive Services and Records Management
Key words	information, library, archive, knowledge, records management