Other Information
Office information systems are opportunities for faster dissemination and sharing of business information using a combination of: documents, computers, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities and facsimile machines.

10.9 Electronic commerce services

Objective: To ensure the security of electronic commerce services, and their secure use.

The security implications associated with using electronic commerce services, including on-line transactions, and the requirements for controls, should be considered. The integrity and availability of information electronically published through publicly available systems should also be considered.

10.9.1 Electronic commerce

Control
Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

Implementation guidance
Security considerations for electronic commerce should include the following:

a) the level of confidence each party requires in each others claimed identity, e.g. through authentication;

b) authorization processes associated with who may set prices, issue or sign key trading documents;

c) ensuring that trading partners are fully informed of their authorisations;

d) determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts, e.g. associated with tendering and contract processes;

e) the level of trust required in the integrity of advertised price lists;

f) the confidentiality of any sensitive data or information;

g) the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts;

h) the degree of verification appropriate to check payment information supplied by a customer;

i) selecting the most appropriate settlement form of payment to guard against fraud;

j) the level of protection required to maintain the confidentiality and integrity of order information;

k) avoidance of loss or duplication of transaction information;

l) liability associated with any fraudulent transactions;

m) insurance requirements.

Many of the above considerations can be addressed by the application of cryptographic controls (see 12.3), taking into account compliance with legal requirements (see 15.1, especially 15.1.6 for cryptography legislation).

Electronic commerce arrangements between trading partners should be supported by a documented agreement which commits both parties to the agreed terms of trading, including details of authorization (see b) above). Other agreements with information service and value added network providers may be necessary.

This is a preview. Click here to purchase the full publication.

Public trading systems should publicize their terms of business to customers.

Consideration should be given to the resilience to attack of the host(s) used for electronic commerce, and the security implications of any network interconnection required for the implementation of electronic commerce services (see 11.4.6).

Other Information
Electronic commerce is vulnerable to a number of network threats that may result in fraudulent activity, contract dispute, and disclosure or modification of information.

Electronic commerce can make use of secure authentication methods, e.g. using public key cryptography and digital signatures (see also 12.3) to reduce the risks. Also, trusted third parties can be used, where such services are needed.

10.9.2 On-Line Transactions

Control
Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Implementation guidance
Security considerations for on-line transactions should include the following:

a) the use of electronic signatures by each of the parties involved in the transaction;

b) all aspects of the transaction, i.e. ensuring that:

   1) user credentials of all parties are valid and verified;

   2) the transaction remains confidential; and

   3) privacy associated with all parties involved is retained;

c) communications path between all involved parties is encrypted;

d) protocols used to communicate between all involved parties is secured;

e) ensuring that the storage of the transaction details are located outside of any public accessible environment, e.g. on a storage platform existing on the organizational Intranet, and not retained and exposed on a storage medium directly accessible from the Internet;

f) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures and/or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

Other Information
The extent of the controls adopted will need to be commensurate with the level of the risk associated with each form of on-line transaction.

Transactions may need to comply with laws, rules, and regulations in the jurisdiction in which the transaction is generated from, processed via, completed at, and/or stored.

There exist many forms of transactions that can be performed in an on-line manner e.g. contractual, financial etc.

This is a preview. Click here to purchase the full publication.

10.9.3 Publicly available information

Control

The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

Implementation guidance

Software, data, and other information requiring a high level of integrity, being made available on a publicly available system, should be protected by appropriate mechanisms, e.g. digital signatures (see 12.3). The publicly accessible system should be tested against weaknesses and failures prior to information being made available.

There should be a formal approval process before information is made publicly available. In addition, all input provided from the outside to the system should be verified and approved.

Electronic publishing systems, especially those that permit feedback and direct entering of information, should be carefully controlled so that:

a) information is obtained in compliance with any data protection legislation (see 15.1.4);

b) information input to, and processed by, the publishing system will be processed completely and accurately in a timely manner;

c) sensitive information will be protected during collection, processing, and storage;

d) access to the publishing system does not allow unintended access to networks to which the system is connected.

Other Information

Information on a publicly available system, e.g. information on a Web server accessible via the Internet, may need to comply with laws, rules, and regulations in the jurisdiction in which the system is located, where trade is taking place or where the owner(s) reside. Unauthorized modification of published information may harm the reputation of the publishing organization.

10.10 Monitoring

Objective: To detect unauthorized information processing activities.

Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified.

An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities.

System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

10.10.1 Audit logging

Control

Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Implementation guidance

Audit logs should include, when relevant:

a) user IDs;

b) dates, times, and details of key events, e.g. log-on and log-off;

This is a preview. Click here to purchase the full publication.

c) terminal identity or location if possible;

d) records of successful and rejected system access attempts;

e) records of successful and rejected data and other resource access attempts;

f) changes to system configuration;

g) use of privileges;

h) use of system utilities and applications;

i) files accessed and the kind of access;

j) network addresses and protocols;

k) alarms raised by the access control system;

l) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

Other information

The audit logs may contain intrusive and confidential personal data. Appropriate privacy protection measures should be taken (see also 15.1.4). Where possible, system administrators should not have permission to erase or de-activate logs of their own activities (see 10.1.3).

10.10.2 Monitoring system use

Control

Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.

Implementation guidance

The level of monitoring required for individual facilities should be determined by a risk assessment. An organisation should comply with all relevant legal requirements applicable to its monitoring activities. Areas that should be considered include:

a) authorized access, including detail such as:
   1) the user ID;
   2) the date and time of key events;
   3) the types of events;
   4) the files accessed;
   5) the program/utilities used;

b) all privileged operations, such as:
   1) use of privileged accounts, e.g. supervisor, root, administrator;
   2) system start-up and stop;
   3) I/O device attachment/detachment;

c) unauthorized access attempts, such as:
   1) failed or rejected user actions;
   2) failed or rejected actions involving data and other resources;
   3) access policy violations and notifications for network gateways and firewalls;
   4) alerts from proprietary intrusion detection systems;

This is a preview. Click here to purchase the full publication.

d) system alerts or failures such as:
   1) console alerts or messages;
   2) system log exceptions;
   3) network management alarms;
   4) alarms raised by the access control system;
e) changes to, or attempts to change, system security settings and controls.

How often the results of monitoring activities are reviewed should depend on the risks involved. Risk factors that should be considered include the:

a) criticality of the application processes;
b) value, sensitivity, and criticality of the information involved;
c) past experience of system infiltration and misuse, and the frequency of vulnerabilities being exploited;
d) extent of system interconnection (particularly public networks);
e) logging facility being de-activated.

Other information
Usage monitoring procedures are necessary to ensure that users are only performing activities that have been explicitly authorized.

A log review involves understanding the threats faced by the system and the manner in which these may arise. Examples of events that might require further investigation in case of information security incidents are given in 13.1.1.

10.10.3 Protection of log information

Control
Logging facilities and log information should be protected against tampering and unauthorized access.

Implementation guidance
Controls should aim to protect against unauthorized changes and operational problems with the logging facility including:

a) alterations to the message types that are recorded;
b) log files being edited or deleted;
c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence (see also 13.2.3).

Other information
System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation and rationalization should be considered.

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security.

This is a preview. Click here to purchase the full publication.

10.10.4 Administrator and operator logs

Control
System administrator and system operator activities should be logged.

Implementation guidance
Logs should include:

a) the time at which an event (success or failure) occurred;

b) information about the event (e.g. files handled) or failure (e.g. error occurred and corrective action taken);

c) which account and which administrator or operator was involved;

d) which processes were involved.

System administrator and operator logs should be reviewed on a regular basis.

Other information
An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

10.10.5 Fault logging

Control
Faults should be logged, analysed, and appropriate action taken.

Implementation guidance
Faults reported by users or by system programs related to problems with information processing or communications systems should be logged. There should be clear rules for handling reported faults including:

a) review of fault logs to ensure that faults have been satisfactorily resolved;

b) review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

It should be ensured that error logging is enabled, if this system function is available.

Other information
Logging of errors and faults can impact the performance of a system. Such logging should be enabled by competent personnel, and the level of logging required for individual systems should be determined by a risk assessment, taking performance degradation into account.

10.10.6 Clock synchronization

Control
The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.

Implementation guidance
Where a computer or communications device has the capability to operate a real-time clock, this clock should be set to an agreed standard, e.g. Coordinated Universal Time (UTC) or local standard time. As some clocks are known to drift with time, there should be a procedure that checks for and corrects any significant variation.

The correct interpretation of the date/time format is important to ensure that the timestamp reflects the real date/time. Local specifics (e.g. daylight savings) should be taken into account.

This is a preview. Click here to purchase the full publication.

Other information

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems. A network time protocol can be used to keep all of the servers in synchronisation with the master clock.

This is a preview. Click here to purchase the full publication.

11 Access control

11.1 Business requirement for access control

Objective: To control access to information.
Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.
Access control rules should take account of policies for information dissemination and authorization.

11.1.1 Access control policy

Control

An access control policy should be established, documented, and reviewed based on business and security requirements for access.

Implementation guidance

Access control rules and rights for each user or group of users should be clearly stated in an access control policy. Access controls are both logical and physical (see also section 9) and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

a) security requirements of individual business applications;

b) identification of all information related to the business applications and the risks the information is facing;

c) policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information (see 7.2);

d) consistency between the access control and information classification policies of different systems and networks;

e) relevant legislation and any contractual obligations regarding protection of access to data or services (see 15.1);

f) standard user access profiles for common job roles in the organization;

g) management of access rights in a distributed and networked environment which recognizes all types of connections available;

h) segregation of access control roles, e.g. access request, access authorization, access administration;

i) requirements for formal authorization of access requests (see 11.2.1);

j) requirements for periodic review of access controls (see 11.2.4);

k) removal of access rights (see 8.3.3).

Other information

Care should be taken when specifying access control rules to consider:

a) differentiating between rules that must always be enforced and guidelines that are optional or conditional;

This is a preview. Click here to purchase the full publication.

b) establishing rules based on the premise "Everything is generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";

c) changes in information labels (see 7.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;

d) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;

e) rules, which require specific approval before enactment, and those which do not.

Access control rules should be supported by formal procedures and clearly defined responsibilities (see, for example, 6.1.3, 11.3, 10.4.1, 11.6).

11.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

Formal procedures should be in place to control the allocation of access rights to information systems and services.

The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

11.2.1 User registration

Control

There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

Implementation guidance

The access control procedure for user registration and de-registration should include:

a) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of group IDs should only be permitted where they are necessary for business or operational reasons, and should be approved and documented;

b) checking that the user has authorization from the system owner for the use of the information system or service; separate approval for access rights from management may also be appropriate;

c) checking that the level of access granted is appropriate to the business purpose (see 11.1) and is consistent with organizational security policy, e.g. it does not compromise segregation of duties (see 10.1.3);

d) giving users a written statement of their access rights;

e) requiring users to sign statements indicating that they understand the conditions of access;

f) ensuring service providers do not provide access until authorization procedures have been completed;

g) maintaining a formal record of all persons registered to use the service;

h) immediately removing or blocking access rights of users who have changed roles or jobs or left the organization;

i) periodically checking for, and removing or blocking, redundant user IDs and accounts (see 11.2.4);

j) ensuring that redundant user IDs are not issued to other users.

This is a preview. Click here to purchase the full publication.

Other information
Consideration should be given to establish user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews (see 11.2.4) are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel or service agents (see also 6.1.5, 8.1.3 and 8.2.3).

11.2.2 Privilege management

Control
The allocation and use of privileges should be restricted and controlled.

Implementation guidance
Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process. The following steps should be considered:

a) the access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated should be identified;

b) privileges should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (11.1.1), i.e. the minimum requirement for their functional role only when needed;

c) an authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete;

d) the development and use of system routines should be promoted to avoid the need to grant privileges to users;

e) the development and use of programs which avoid the need to run with privileges should be promoted;

f) privileges should be assigned to a different user ID from those used for normal business use.

Other information
Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) can be a major contributory factor to the failures or breaches of systems.

11.2.3 User password management

Control
The allocation of passwords should be controlled through a formal management process.

Implementation guidance
The process should include the following requirements:

a) users should be required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group; this signed statement could be included in the terms and conditions of employment (see 8.1.3);

This is a preview. Click here to purchase the full publication.

b) when users are required to maintain their own passwords they should be provided initially with a secure temporary password (see 11.3.1), which they are forced to change immediately;

c) establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;

d) temporary passwords should be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided;

e) temporary passwords should be unique to an individual and should not be guessable;

f) users should acknowledge receipt of passwords;

g) passwords should never be stored on computer systems in an unprotected form;

h) default vendor passwords should be altered following installation of systems or software.

Other information

Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorization. Other technologies for user identification and authentication, such as biometrics, e.g. finger-print verification, signature verification, and use of hardware tokens, e.g. smart cards, are available, and should be considered if appropriate.

11.2.4 Review of user access rights

Control

Management should review users' access rights at regular intervals using a formal process.

Implementation guidance

The review of access rights should consider the following guidelines:

a) users' access rights should be reviewed at regular intervals, e.g. a period of 6 months, and after any changes, such as promotion, demotion, or termination of employment (see 11.2.1);

b) user access rights should be reviewed and re-allocated when moving from one employment to another within the same organization;

c) authorizations for special privileged access rights (see 11.2.2) should be reviewed at more frequent intervals, e.g. at a period of 3 months;

d) privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained;

e) changes to privileged accounts should be logged for periodic review.

Other information

It is necessary to regularly review users' access rights to maintain effective control over access to data and information services.

11.3 User responsibilities

Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

The co-operation of authorized users is essential for effective security.

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

A clear desk and clear screen policy should be implemented to reduce the risk of unauthorized access or damage to papers, media, and information processing facilities.

This is a preview. Click here to purchase the full publication.