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. Other agreements with information service and value added network providers may be necessary.

Consideration should be given to the resilience to attack of the host used for electronic commerce and the security implications of any network interconnection required for its implementation.

7.7 Mobile Computing

Formal procedures must be in place and appropriate controls must be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments. For example such procedures should include the requirements for:

- physical protection,
- access controls,
- cryptographic techniques,
- back-ups, and
- virus protection.

Procedures should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques.

It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date. Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, e.g., theft or loss of information.

Suitable protection should be given to the use of mobile facilities connected to networks.

Remote access to business information across public network using mobile computing facilities should only take place after successful identification and authentication and with suitable access control mechanisms in place.

Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. Equipment carrying important, sensitive and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment.

7.8 Remote Computing

Remote computing uses communications technology to enable staff or agencies to work remotely from a fixed location outside of their organization. Suitable protection of the remote computing site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. It is important that remote computing is both authorized and controlled by management and that suitable arrangements are in place for this way of working.

Procedures must be developed from best practices to authorize and control remote computing activities. Agencies should only authorize remote computing activities if they are satisfied that appropriate security arrangements and controls are in place and that these comply with the agency's security procedures. The following should be considered:

- the existing physical security of the remote computing site, taking into account the physical security of the building and the local environment,
- the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system, and
- the threat of unauthorized access to information or resources from other people using the accommodation.

The controls and arrangements to be considered include:

- the provision of suitable equipment and storage furniture for the remote computing activities,
- a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the user is authorized to access,
- the provision of suitable communication equipment, including methods for securing remote access,
- physical security,
- the provision of hardware and software support and maintenance,
- the procedures for back-up and business continuity, and
- audit and security monitoring.

7.9 External Facilities

The use of an external contractor to manage information processing or communication facilities may introduce potential security exposures, such as the possibility of compromise, damage or loss of data at the contractor's site.

Prior to using external facilities, the risks must be identified and appropriate controls agreed with the contractor and incorporated into the contract. Particular issues that should be addressed include:

- identifying sensitive or critical applications better retained in-house,
- obtaining the approval of business application owners,

- implications for business continuity plans,
- security standards to be specified and the process for measuring compliance,
- allocation of specific responsibilities and procedures to effectively monitor all relevant security activities, and
- responsibilities and procedures for reporting and handling security incidents.

7.10 Encryption

Encryption should be applied to protect the confidentiality of sensitive or critical information.

Based on a risk assessment, the required level of protection should be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys to be used.

Specialist advice should be sought to identify the appropriate level of protection, to select suitable products that will provide the required protection and the implementation of a secure system of key management. In addition, legal advice may need to be sought regarding the laws and regulations that might apply to the organization's intended use of encryption.

Procedures for the use of cryptographic controls for the protection of information must be developed and followed. Such procedures are necessary to maximize benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

When developing procedures the following should be considered:

- the management guidelines on the use of cryptographic controls across the organization,
- including the general principles under which business information should be protected,
- the approach to key management, including methods to deal with the recovery of encrypted information in the case of lost, compromised or damaged keys,
- roles and responsibilities, e.g. who is responsible for: the implementation of the procedures; the key management,
- how the appropriate level of cryptographic protection is to be determined, and
- the standards to be adopted for the effective implementation throughout the organization (which solution is used for which business processes).