



## **MANAGED SERVICE PROVIDER (MSP) PROGRAM**

### **SECURITY POLICY FOR DATA MANAGEMENT AND PERSONNEL**

***JUNE, 2001***

# TABLE OF CONTENTS

Chapter 1 – SECURING HARDWARE, PERIPHERALS AND OTHER EQUIPMENT .....	1
<i>Purchasing and Installing Hardware</i> .....	1
<i>Cabling, UPS, Printers and Modems</i> .....	1
<i>Consumables</i> .....	1
<i>Working Off Premises or Using Outsourced Processing</i> .....	1
<i>Using Secure Storage</i> .....	2
<i>Using Lockable Filing Cabinets</i> .....	2
<i>Using Fire Protected Storage Cabinets</i> .....	2
<i>Using a Safe</i> .....	2
<i>Documenting Hardware</i> .....	2
<i>Other Hardware Issues</i> .....	2
Chapter 2 – CONTROLLING ACCESS TO INFORMATION AND SYSTEMS .....	4
<i>Managing Access Control Standards</i> .....	4
<i>Managing User Access</i> .....	4
<i>Securing Unattended Workstations</i> .....	4
<i>Managing Network Access Controls</i> .....	4
<i>Controlling Access to Operating System Software</i> .....	4
<i>Managing Passwords</i> .....	4
<i>Securing Against Unauthorized Physical Access</i> .....	4
<i>Restricting Access</i> .....	4
<i>Monitoring System Access and Use</i> .....	4
<i>Giving Access to Files and Documents</i> .....	4
<i>Managing Higher Risk System Access</i> .....	5
<i>Controlling Remote User Access</i> .....	5
Chapter 3 – PROCESSING INFORMATION AND DOCUMENTS .....	6
<i>Networks</i> .....	6
<i>Managing the Network</i> .....	6
<i>Accessing your Network Remotely</i> .....	6
<i>Defending your Network Information from Malicious Attack</i> .....	6
<i>System Operations and Administration</i> .....	6
<i>Administrating Systems</i> .....	6
<i>Controlling Data Distribution</i> .....	6
<i>Permitting Third Party Access</i> .....	6
<i>Managing Electronic Keys</i> .....	6
<i>Managing System Operations and System Administration</i> .....	6
<i>Managing System Documentation</i> .....	7
<i>Monitoring Error Logs</i> .....	7
<i>Scheduling Systems Operations</i> .....	7
<i>Scheduling Changes to Routine Systems Operations</i> .....	7
<i>E-mail and the Worldwide Web</i> .....	7
<i>Telephones &amp; Fax</i> .....	8
<i>Transferring and Exchanging Data</i> .....	9
<i>Managing Data Storage</i> .....	9
<i>Receiving Information on Disks</i> .....	9
<i>Information Retention Policy</i> .....	9
<i>Backup, Recovery and Archiving</i> .....	10
<i>Document Handling</i> .....	10
<i>Securing Data</i> .....	11
<i>Other Information Handling and Processing</i> .....	12
Chapter 4 – PURCHASING AND MAINTAINING COMMERCIAL SOFTWARE .....	13
<i>Purchasing and Installing Software</i> .....	13
<i>Software Maintenance &amp; Upgrade</i> .....	13
<i>Other Software Issues</i> .....	13
Chapter 5 – DEVELOPING AND MAINTAINING IN-HOUSE SOFTWARE .....	14



<i>Controlling Software Code</i> .....	14
<i>Software Development</i> .....	14
<i>Testing &amp; Training</i> .....	14
<i>Documentation</i> .....	15
<i>Other Software Development</i> .....	15
Chapter 6 – COMBATING CYBER CRIME .....	16
<i>Combating Cyber Crime</i> .....	16
Chapter 7 – COMPLYING WITH LEGAL AND POLICY REQUIREMENTS .....	17
<i>Complying with Legal Obligations</i> .....	17
<i>Complying with Policies</i> .....	17
<i>Avoiding Litigation</i> .....	17
<i>Other Legal Issues</i> .....	17
Chapter 8 – PLANNING FOR BUSINESS CONTINUITY .....	19
<i>Business Continuity Management (BCP)</i> .....	19
Chapter 9 – ADDRESSING PERSONNEL ISSUES RELATING TO SECURITY .....	20
<i>Contractual Documentation</i> .....	20
<i>Confidential Personnel Data</i> .....	20
<i>Handling Confidential Employee Information</i> .....	20
<i>Personnel Information Security Responsibilities</i> .....	20
<i>HR Management</i> .....	21
<i>Staff Leaving Employment</i> .....	21
<i>HR Issues Other</i> .....	22
Chapter 10 – CONTROLLING E-COMMERCE INFORMATION SECURITY .....	23
<i>E-Commerce Issues</i> .....	23
Chapter 11 – DELIVERING TRAINING AND STAFF AWARENESS .....	24
<i>Awareness</i> .....	24
<i>Training</i> .....	24
Chapter 12 – DEALING WITH PREMISES RELATED CONSIDERATIONS.....	25
<i>Premises Security</i> .....	25
<i>Data Stores</i> .....	25
<i>Other Premises Issues</i> .....	25
Chapter 13 – DETECTING AND RESPONDING TO IS INCIDENTS .....	26
<i>Reporting Information Security Incidents</i> .....	26
<i>Investigating Information Security Incidents</i> .....	26
<i>Corrective Activity</i> .....	26
<i>Other Information Security Incident Issues</i> .....	26
Chapter 14 – CLASSIFYING INFORMATION AND DATA.....	28
<i>Setting Classification Standards</i> .....	28



## *Chapter 1*

# SECURING HARDWARE, PERIPHERALS AND OTHER EQUIPMENT

### ***Purchasing and Installing Hardware***

All purchases of new systems hardware or new components for existing systems must be made in accordance with Information Security and other organization Policies, as well as technical standards. Such requests to purchase must be based upon a 'User Requirements Specification' document and take account of longer-term organizational business needs.

Except for minor purchases, hardware must be purchased through a structured evaluation process, which must include the development of a detailed 'Request For Proposal' (RFP) document. Information Security features and requirements must be identified within the RFP.

All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date. Information Security requirements for new installations are to be circulated for comment to all interested parties, well in advance of installation.

All equipment must be fully and comprehensively tested and formally accepted by users before being transferred to the 'live' environment.

### ***Cabling, UPS, Printers and Modems***

An 'Uninterruptible Power Supply' is to be installed to ensure the continuity of services during power outages.

Secondary and backup power generators are to be employed where necessary to ensure the continuity of services during power outages.

Sensitive or confidential information may only be faxed where more secure methods of transmission are not feasible. Both the owner of the information and the intended recipient must authorize the transmissions beforehand.

Sensitive or confidential information may only be sent via public telephone lines where more secure methods of transmission are not feasible. Both the owner and the recipient must authorize the transmission beforehand.

Information 'classified' as Highly Confidential or Top Secret, may never be sent to a network printer without there being an authorized person to safeguard its confidentiality during and after printing.

Network cabling should be installed and maintained by qualified engineers to ensure the integrity of both the cabling and the wall-mounted sockets. Any unused network wall sockets should be sealed-off and their status formally noted.

### ***Consumables***

IT consumables must be purchased in accordance with the organization's approved purchasing procedures with usage monitored to discourage theft and improper use.

Only personnel who are authorized to install or modify software shall use removable media to transfer data to/from the organization's network. Any other persons shall require specific authorization.

### ***Working Off Premises or Using Outsourced Processing***

Persons responsible for commissioning outsourced computer processing must ensure that the services used are from reputable companies that operate in accordance with quality standards which should include a suitable 'Service Level Agreement' which meets the organization's requirements.



Line management must authorize the issue of portable computers. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices.

Persons who are issued portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implementing the appropriate safeguards to minimize the risks.

Off-site computer usage, whether at home or at other locations, may only be used with the authorization of line management. Usage is restricted to business purposes, and users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate security measures.

Any movement of hardware between the organization's locations is to be strictly controlled by authorized personnel.

Personnel issued with mobile phones by the organization are responsible for using them in a manner consistent with the confidentiality level of the matters being discussed.

Personnel using business centers to work on the organization's business are responsible for ensuring the security and subsequent removal and deletion of any information entered into the business center's systems.

Laptop computers are to be issued to, and used only by, authorized employees and only for the purpose for which they are issued. The information stored on the laptop is to be suitably protected at all times.

### ***Using Secure Storage***

Using Lockable Storage Cupboards

Sensitive or valuable material and equipment must be stored securely and according to the classification status of the information being stored.

### ***Using Lockable Filing Cabinets***

Documents are to be stored in a secure manner in accordance with their classification status.

### ***Using Fire Protected Storage Cabinets***

Documents are to be stored in a secure manner in accordance with their classification status.

### ***Using a Safe***

Documents are to be stored in a secure manner in accordance with their classification status.

### ***Documenting Hardware***

Hardware documentation must be kept up-to-date and readily available to the staff who are authorized to support or maintain systems.

A formal 'Hardware Inventory' of all equipment is to be maintained and kept up to date at all times.

### ***Other Hardware Issues***

Equipment owned by the organization may only be disposed of by authorized personnel who have ensured that the relevant security risks have been mitigated.

All information system hardware faults are to be reported promptly and recorded in a hardware fault register.



All computing equipment and other associated hardware belonging to the organization must carry appropriate insurance cover against hardware theft, damage, or loss.

All portable computing equipment is to be insured to cover travel domestically or abroad.

All users of workstations, PCs/laptops are to ensure that their screens are clear/blank when not being used.

Approved login procedures must be strictly observed and users leaving their screen unattended must first lock access to their workstation or log off.

Sensitive or confidential information must not be recorded on Answering Machine/Voice Mail systems.

Only authorized personnel are permitted to take equipment belonging to the organization off the premises; they are responsible for its security at all times.

All equipment owned, leased or licensed by the organization must be supported by appropriate maintenance facilities from qualified engineers.

All speed dialing systems must incorporate security features, which protect sensitive or confidential information.

Only suitable and approved cleaning materials are to be used on equipment owned by the organization.

Deliberate or accidental damage to organization property must be reported to the nominated Information Security Officer as soon as it is noticed.



## *Chapter 2*

# CONTROLLING ACCESS TO INFORMATION AND SYSTEMS

### ***Managing Access Control Standards***

Access control standards for information systems must be established by management and should incorporate the need to balance restrictions to prevent unauthorized access against the need to provide unhindered access to meet business needs.

### ***Managing User Access***

The owner of the system must authorize access to all systems and such access, including the appropriate access rights (or privileges) must be recorded in an Access Control List. Such records are to be regarded as Highly Confidential documents and safeguarded accordingly.

### ***Securing Unattended Workstations***

Equipment is always to be safeguarded appropriately – especially when left unattended.

### ***Managing Network Access Controls***

Access to the resources on the network must be strictly controlled to prevent unauthorized access.

Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

### ***Controlling Access to Operating System Software***

Access to operating system commands is to be restricted to those persons who are authorized to perform systems administration/management functions. Even then, such access must be operated under dual control requiring specific approval of senior management.

### ***Managing Passwords***

The selections of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords shall not be shared with any other person for any reason.

### ***Securing Against Unauthorized Physical Access***

Physical access to high security areas is to be controlled with strong identification and authentication techniques. Staff with authorization to enter such areas are to be provided with information on the potential security risks involved.

### ***Restricting Access***

Access controls are to be set at an appropriate level, which minimizes information security risks, yet also allows the organization's business activities to be carried without undue hindrance.

### ***Monitoring System Access and Use***

Access is to be logged and monitored to identify potential misuse of systems or information.

### ***Giving Access to Files and Documents***

Access to information and documents is to be carefully controlled, ensuring that only authorized personnel may have access to sensitive information.



### ***Managing Higher Risk System Access***

Access controls for highly sensitive information or high risk systems are to be set in accordance with the value and classification of the information assets being protected.

### ***Controlling Remote User Access***

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques.

### ***Networks***

The network must be designed and configured to deliver high performance and reliability to meet the needs of the business while providing a high degree of 'access control' and a range of 'privilege' restrictions.

### ***Managing the Network***

Suitably qualified staff are to manage the organization's network, and preserve its integrity in collaboration with the nominated individual system owners.

### ***Accessing your Network Remotely***

Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

### ***Defending your Network Information from Malicious Attack***

System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

### ***System Operations and Administration***

The organization's systems are to be managed by a suitably qualified 'systems administrator' who is responsibly for overseeing the day-to-day running and security of the systems.

### ***Administrating Systems***

System Administrator must be fully trained and have adequate experience in the wide range of systems and platforms used by the organization. In addition, they must be knowledgeable and conversant with the range of Information Security risks, which need to be managed.

### ***Controlling Data Distribution***

For authorized personnel, the appropriate data and information must be made available as and when required; for all other persons, access to such data and information is prohibited with appropriate technical control required to supplement the enforcement of this policy.

### ***Permitting Third Party Access***

Third party access to corporate information is only permitted where the information in question has been 'ring fenced' and the risk of possible unauthorized access is considered to be negligible.

### ***Managing Electronic Keys***

The management of electronic keys to control both the encryption and decryption of sensitive messages must be performed under dual control, with duties being rotated between staff.

### ***Managing System Operations and System Administration***

The organization's systems must be operated and administered using documented procedures in a manner, which is both efficient but also effective in protecting the organization's information security.



## ***Managing System Documentation***

System documentation is a requirement for all the organization's information systems. Such documentation must be kept up-to-date and be available.

## ***Monitoring Error Logs***

Error logs must be properly reviewed and managed by qualified staff.

## ***Scheduling Systems Operations***

Systems Operations schedules are to be formally planned, authorized and documented.

## ***Scheduling Changes to Routine Systems Operations***

Changes to routine systems operations are to be fully tested and approved before being implemented.

Operational 'audit logs' are to be reviewed regularly by trained staff and discrepancies reported to the owner of the information systems.

System clocks must be synchronized regularly especially between the organization's various processing 'platforms'.

Only qualified and authorized staff or approved third party technicians may repair information system hardware faults.

Transaction and processing reports should be regularly reviewed by properly trained and qualified staff.

Any Facilities Management company must be able to demonstrate compliance with this organization's Information Security Policies and also provide a 'Service Level Agreement' which documents the performance expected and the remedies available in case of non compliance.

## ***E-mail and the Worldwide Web***

Great care must be taken when downloading information and files from the Internet to safeguard against both 'malicious code' and also inappropriate material.

The transmission of sensitive and confidential data is to be 'authenticated' by the use of 'digital signatures' whenever possible.

E-mail should only be used for business purposes, using terms, which are consistent with other forms of business communication. The attachment of data files to an email is only permitted after confirming the 'classification' of the information being sent and then having scanned and verified the file for the possibility of a 'virus' or other 'malicious code'.

Incoming e-mail must be treated with the utmost care due to its 'inherent Information Security risks'. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible 'viruses' or other 'malicious code'.

Data retention periods for e-mail must be established to meet legal and business requirements and must be adhered to by all staff.

Persons responsible for setting up Intranet access must ensure that any 'access restrictions' pertaining to the data in source systems, are also applied to access from the organization's Intranet.

Persons responsible for setting up Extranet access must ensure that any 'access restrictions' pertaining to the data in source systems, are also applied to access from the organization's Extranet.



Persons responsible for setting up Internet access are to ensure that the organization's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured 'firewall'. Human Resources management must ensure that all personnel with Internet access (including e-mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet in addition to compliance with the organization's Information Security Policies.

Due to the signification risk of malicious intrusion from unauthorized external persons, Web sites may only be developed and maintained by properly qualified and authorized personnel.

Unsolicited e-mail is to be treated with caution and not responded to.

Ensure that information you are forwarding by e-mail (especially attachments) is correctly addressed and only being sent to appropriate persons.

Management is responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security incidents.

Staff authorized to make payment by credit card for goods ordered on the Internet, are responsible for its safe and appropriate use.

Web browsers are to be used in a secure manner by making use of the built-in security features of the software concerned. Management must ensure that staff is made aware of the appropriate settings for the software concerned.

Information obtained from Internet sources should be verified before used for business purposes.

The Web site is an important marketing and information resource for the organization, and its safety from unauthorized intrusion is a top priority. Only qualified authorized persons may amend the Web site with all changes being documented and reviewed.

The organization will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by staff. Reports of attempted access will be scrutinized by management on a regular basis.

Computer files received from unknown senders are to be deleted without being opened.

### ***Telephones & Fax***

Conference calls are only permitted if staff are aware of the Information Security issues involved.

Video conference calls are only permitted if staff are aware of the Information Security issues involved.

All parties are to be notified in advance whenever telephone conversations are to be recorded.

Any fax received in error is to be returned to the sender. Its contents must not be disclosed to other parties without the sender's permission.

Staff authorized to make payment by credit card for goods ordered over the telephone, are responsible for safe and appropriate use.

The identity of recipients of sensitive or confidential information over the telephone must be verified.

The identity of persons requesting sensitive or confidential information over the telephone must be verified, and they must be authorized to receive it.

Unsolicited or unexpected faxes should be treated with care until the sender has been identified.



## ***Transferring and Exchanging Data***

Sensitive or confidential data/information, may only be transferred across networks, or copies to other media, when the confidentiality and integrity of the data can be reasonably assured e.g. by using encryption techniques.

## ***Managing Data Storage***

Day-to-day storage must ensure that current data is readily available to authorized users and that archives are both created and accessible in case of the need.

The integrity and stability of the organization's databases must be maintained at all times.

Emergency data amendments may only be used in extreme circumstances and only in accordance with emergency amendment procedures.

## ***Receiving Information on Disks***

The use of removable media disks e.g. disks and CD-ROMS is not permitted except where specifically authorized.

Data directories and structures should be established by the owner of the information system with users adhering to that structure. Access restrictions to such directories should be applied as necessary to restrict unauthorized access.

Existing directory and folder structures may only be amended with the appropriate authorization, usually from the owner of the information system concerned.

The archiving of documents must take place with due consideration for legal, regulatory and business issues with liaison between technical and business staff.

## ***Information Retention Policy***

The information created and stored by the organization's information systems must be retained for a minimum period that meets both legal and business requirements.

The classification of spreadsheets must be appropriate to the sensitivity and confidentiality of data contained therein. All financial/data models used for decision-making are to be fully documented and controlled by the information owner.

Databases must be fully tested for both business logic and processing, prior to operational usage. Where such databases are to contain information of a personal nature, procedures and access controls must ensure compliance with necessary legislation e.g. 'Data Protection'.

Highly sensitive or critical documents must not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports must be self contained and contain all the necessary information.

Draft reports should only be updated with the authority of the designated owner of the report.

Draft version(s) of reports must be deleted or archived following production of a final version. A single version of the file should be retained for normal operational access.

Version control procedures should always be applied to documentation belonging to the organization or its customers.

Only authorized persons may access the sensitive or confidential data on projects owned or managed by the organization or its employees.



Customer information may only be updated by authorized personnel. Customer data is to be safeguarded using a combination of technical access controls and robust procedures, with all changes supported by journals and internal audit controls.

The naming of the organization's data files must be meaningful and capable of being recognized by its intended users.

A document's security 'classification' level and ownership should be stated within the header and footer space on each page of all documents.

Temporary files on users' PCs and laptops are to be deleted regularly to prevent possible misuse by possible unauthorized users.

Customer contact information is to be 'classified' as Highly Confidential and secured accordingly.

All users of information systems whose job function requires them to create or amend data files, must save their work on the system regularly in accordance with best practice, to prevent corruption or loss through system or power malfunction.

### ***Backup, Recovery and Archiving***

Information system owners must ensure that adequate back up and system recovery procedures are in place.

Information and data stored on Laptop and portable computers must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

Backup of the organization's data files and the ability to recover such data is a top priority. Management are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.

The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved.

The archiving of electronic data files must reflect the needs of the business and also any legal and regulatory requirements.

Management must ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files; especially where such files may replace more recent files.

### ***Document Handling***

Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorization levels specified for those documents.

All employees to be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents. Authorization from the document owner should be obtained where documents are 'classified' as Highly Confidential or above.

All information used for, or by the organization, must be filed appropriately and according to its 'classification'.

Documents should be countersigned (either manually or electronically) to confirm their validity and integrity; especially those which commit or oblige the organization in its business activities.

Documents should be checked to confirm their validity and integrity; especially those which commit or oblige the organization in its business activities.

All written communications sent out by the organization to third parties are to be approved by authorized persons.



All signatures authorizing access to systems or release of information must be properly authenticated.

Unsolicited mail should not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified.

An agreed 'corporate' document style should be used which promotes consistency, integrity and promotes the agreed 'image' of the organization.

The designated owners of documents which contain sensitive information are responsible for ensuring that the measures taken to protect their 'confidentiality, integrity and availability', during and after transportation/transmission, are adequate and appropriate.

All documents of a sensitive or 'confidential nature' are to be shredded when no longer required. The document owner must authorize or initiate this destruction.

All users of information systems must manage the creation, storage, amendment, copying and deletion/destruction of data files in a manner which safeguards and protects the 'confidentiality, integrity and availability' of such files'. The degree to which software techniques and disciplined user procedures are necessary will be applied by management and determined by the 'classification' of the information/data in question.

### ***Securing Data***

Where appropriate, sensitive or 'confidential' information or data should always be transmitted in 'encrypted' form. Prior to transmission, consideration must always be given to the procedures to be used between the sending and recipient parties and any possible legal issues from using encryption techniques.

Persons responsible for Human Resources Management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organization and to external parties.

Prior to sending information to third parties, not only must the intended recipient be authorized to receive such information, but the procedures and Information Security measures adopted by the third party, must be seen to continue to assure the confidentiality and integrity of the information.

Information relating to the clients and third party contacts of the organization is confidential, and must be protected and safeguarded from unauthorized access and disclosure.

Customer credit card details entrusted to the organization must be afforded a combination of security measures (technology and procedural) which, in combination, prevent all recognized possibilities of the card details being accessed, stolen, modified or in any other way divulged to unauthorized persons.

All data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the 'value' and 'classification' of the information being safeguarded.

Prior to sending reports to third parties, not only must the intended recipient(s) be authorized to receive such information, but the procedures and Information Security measures adopted by each third party, must be seen to continue to assure the 'confidentiality and integrity' of the information.

Sensitive financial information is to be 'classified' as Highly Confidential and must be afforded security measures (technology and procedural) which, in combination, safeguard such information from unauthorized access and disclosure.

Data is to be protected against unauthorized or accidental changes, and may only be deleted with the proper authority.

Sensitive/confidential electronic data and information should be secured, whenever possible, with 'access control' applied to the directory on the (computer) system concerned. The sole use of passwords to secure individual



documents is less effective, and hence discouraged, as passwords may either be forgotten or become revealed (over time) to unauthorized persons.

Information 'classified' as Highly Confidential or Top Secret, may never be sent to a network printer without there being an authorized person to retrieve it and hence safeguard its confidentiality during an after printing.

### ***Other Information Handling and Processing***

The decision whether 'dual control' is required for data entry is to be made by the information system owner. Where so required, secure data handling procedures including dual input are to be strictly adhered to.

Employees are not permitted to load non-approved screen savers onto the organization's PCs, laptops and workstations.

Any third party used for external disposal of the organization's obsolete equipment and material must be able to demonstrate compliance with this organization's Information Security Policies and also, where appropriate, provide a 'Service Level Agreement' which documents the performance expected and the remedies available in case of non compliance.

The use of photocopiers or duplicators for personal use is discouraged. In exceptions, specific permission may be given by the employee's immediate supervisor or manager.

Only authorized personnel may speak to the media (newspapers, television, radio, magazines, etc.) about matters relating to the organization.

Information regarding the organization's customers or other people dealing with the organization is to be kept confidential at all times. The information should only be released by authorized and trained persons.

The techniques of 'dual control' and 'segregation of duties' are to be employed to enhance the control over procedures wherever both the risk from, and consequential impact of, a related Information Security 'incident' would likely result in financial or other material damage to the organization.

This organization expects all employees to operate a clear desk policy.

E-mail addresses and faxes are to be checked carefully prior to dispatch, especially where the information is considered to be confidential; and where the disclosure of the e-mail addresses or other contact information to the recipients is a possibility.

The organization values the integrity and correctness of all its business and related information and requires management to develop and adopt the appropriate procedures in this regard.

Employees traveling on business are responsible for the security of information in their custody.

Credit may only be advanced to customers once credit limits have been properly approved, in accordance with the organization's usual financial credit control procedures.



### ***Purchasing and Installing Software***

All requests for new applications systems or software enhancements must be presented to senior management with a 'Business Case' with the business requirements presented in a 'User Requirements Specification' document.

The organization should generally avoid the selection of business critical software which, in the opinion of management, has not been adequately proven by early adopters of the system. The selection process for all new business software must additionally incorporate the criteria upon which the selection will be made. Such criteria must receive the approval of senior management.

All office software packages must be compatible with the organization's preferred and approved computer 'operating system' and 'platform'.

To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all 'End User License Agreements' are to be strictly adhered to.

The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased Information Security risks associated with such projects are mitigated using a combination of procedural and technical control techniques.

### ***Software Maintenance & Upgrade***

Patches to resolve software 'bugs' may only be applied where verified as necessary and with management authorization. They must be from a reputable source and are to be thoroughly 'tested' before use.

Upgrades to software must be properly 'tested' by qualified personnel before they are used in a 'live environment'.

The decision whether to upgrade software is only to be taken after consideration of the associated risks of the upgrade and weighing these against the anticipated benefits and necessity for such change.

Developing Interfacing software systems is a highly technical task and should only be undertaken in a planned and controlled manner by properly qualified personnel.

All application software must be provided with the appropriate level of technical support to ensure that the organization's business is not compromised by ensuring that any software problems are handled efficiently with their resolution available in an acceptable time.

Necessary upgrades to the 'Operating System' of any of the organization's computer systems must have the associated risks identified and be carefully planned, incorporating tested fall-back procedures. All such upgrades being undertaken as a formal project.

Operating Systems must be regularly monitored and all required 'housekeeping' routines adhered to.

Software faults are to be formally recorded and reported to those responsible for software support/maintenance.

### ***Other Software Issues***

The disposal of software should only be taken when it is formerly agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time.



### ***Controlling Software Code***

Only designated staff may access operational program libraries. Amendments may only be made using a combination of technical 'access controls' and robust procedures operated under 'dual control'.

Only designated staff may access program source libraries. Amendments may only be made using a combination of technical 'access controls' and robust procedures operated under 'dual control'.

Formal 'change control' procedures must be utilized for all changes to systems. All changes to programs must be properly authorized and 'tested' before moving to the 'live' environment.

Program listings must be controlled and kept fully up to date at all times.

Formal 'change control' procedures with comprehensive 'audit trails' are to be used to control Program Source Libraries.

Formal 'change control' procedures with comprehensive 'audit trails' are to be used to control versions of old programs.

### ***Software Development***

Software developed for or by the organization must always follow a formalized development process, which itself is managed under the project in question. The integrity of the organization's operational software code must be safeguarded using a combination of technical 'access controls' and restricted 'privilege' allocation and robust procedures.

Emergency amendments to software are to be discouraged, except in circumstances previously designated by management as 'critical'. Any such amendments must strictly follow agreed 'change control' procedures.

All proposed system enhancements must be business driven and supported by an agreed 'Business Case'. Ownership (and responsibility) for any such enhancements will intimately rest with the business owner of the system.

The development of bespoke software is only to be considered, if warranted by a strong 'Business Case' and supported both by management and adequate resources over the projected life and time of the resultant project.

Formal 'change control' procedures must be utilized for all amendments to systems. All changes to programs must be properly authorized and 'tested' in a test environment before moving to the 'live' environment.

Management must ensure that the proper 'segregation of duties' applies to all areas dealing with 'systems development, systems operation, or systems administration'.

### ***Testing & Training***

Formal 'change control' procedures must be employed for all amendments to systems. All changes to programs must be properly authorized and 'tested' in a test environment before moving to the 'live' environment.

The use of live data for 'testing' new system or system changes may only be permitted where adequate controls for security of the data are in place.

Formal 'change control' procedures must be utilized for all amendments to systems. All changes to programs must be properly authorized and tested in a test environment before moving to the 'live' environment.



New systems must be tested for 'capacity', peak 'loading' and 'stress testing'. They must demonstrate a level of performance and 'resilience', which meets or exceeds the technical and business needs and requirements of the organization.

Normal 'System Testing' procedures will incorporate a period of 'parallel running' prior to the new or amended system being acceptable for use in the live environment. The results of parallel running should not reveal problems or difficulties which were not previously passed during 'User Acceptance Testing'.

Training is to be provided to users and technical staff in the functionality and operations of all new systems.

### ***Documentation***

All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the 'live' environment unless supporting documentation is available.

### ***Other Software Development***

Vendor developed software must meet the 'User Requirements Specification' and offer appropriate product support.



## Chapter 6 COMBATING CYBER CRIME

### *Combating Cyber Crime*

Security on the network is to be maintained at the highest level. Those responsible for the network and external communications are to receive proper training in risk assessment and how to build secure systems which minimize the threats from 'cyber crime'.

Plans are to be prepared, maintained and regularly tested to ensure that damage done by possible external 'cyber crime' attacks can be minimized and that restoration takes place as quickly as possible.

Perpetrators of 'cyber crime' will be prosecuted by the organization to the full extent of the law. Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence.

In order to reduce the incidence and possibility of internal attacks, 'access control' standards and 'data classification' standards are to be periodically reviewed while maintained at all times.

It is a priority to minimize the opportunities for 'cyber crime' attacks on the organization's systems and information through a combination of technical 'access controls' and robust procedures.

Contingency plans for a 'denial of service' attack are to be maintained and periodically tested to ensure adequacy.

Risks to the organization's systems and information are to be minimized by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices.

Procedures to deal with hoax 'virus' warnings are to be implemented and maintained.

Without exception, Anti 'Virus' software is to be deployed across all PCs with regular virus definition updates and scanning across both servers, PCs and laptop computers.

The threat posed by the infiltration of a 'virus' is high, as is the risk to the organization's systems and data files. Formal procedures for responding to a virus incident are to be developed, tested and implemented. Virus Incident response must be regularly reviewed and tested.

Anti Virus software must be chosen from a proven leading supplier.

## *Chapter 7*

# COMPLYING WITH LEGAL AND POLICY REQUIREMENTS

### ***Complying with Legal Obligations***

Persons responsible for Human Resources Management are to ensure that all employees are fully aware of their legal responsibilities with respect to their use of computer based information systems and data. Such responsibilities are to be included within key staff documentation such as Terms and Conditions of Employment and the Organization Code of Conduct.

The organization intends to fully comply with the requirements of 'Data Protection legislation' in so far as it directly affects the organization's activities.

Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Copyright, Design and Patents Act legislation (or its equivalent), in so far as these requirements impact on their duties.

Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Copyright and Rights in Database Regulations legislation (or its equivalent), in so far as these requirements impact on their duties.

Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of 'Software Copyright and Licensing' legislation, in so far as these requirements impact on their duties.

Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Computer Misuse legislation (or its equivalent), in so far as these requirements impact on their duties.

### ***Complying with Policies***

The organization will maintain a suitable archiving and record retention procedure.

All employees are required to fully comply with the organization's Information Security policies. The monitoring of such compliance is the responsibility of management.

### ***Avoiding Litigation***

Employees are prohibited from writing derogatory remarks about other persons or organizations.

Information from the Internet or other electronic sources may not be used without authorization from the owner of the 'copyright'.

Information from the Internet or other electronic sources may not be retransmitted without permission from the owner of the 'copyright'.

Text from reports, books or documents may not be reproduced or reused without permission from the 'copyright' owner.

### ***Other Legal Issues***

All employees are to be aware that evidence of 'Information Security incidents' must be formally recorded and retained and passed to the appointed Information Security Officer.



Registered domain names, whether or not actually used for the organization's Web sites, are to be protected and secured in a similar manner to any other valuable asset of the organization.

A re-assessment of the threats and risks involved relating to the organization's business activities must take place periodically to ensure that the organization is adequately insured at all times.

All parties are to be notified in advance whenever conversations are being recorded.



***Business Continuity Management (BCP)***

Management is required to initiate a 'Business Continuity Plan'.

Management is to undertake a formal risk assessment in order to determine the requirements for a 'Business Continuity Plan'.

Management is to develop a 'Business Continuity Plan', which covers all essential and critical business activities.

The 'Business Continuity Plan' is to be periodically tested to ensure that the management and staff understand how it is to be executed.

All staff must be made aware of the 'Business Continuity Plan' and their own respective roles.

The 'Business Continuity Plan' is to be kept up to date and re-tested periodically.

***Contractual Documentation***

The Terms and Conditions of Employment of this organization are to include requirements for compliance with Information Security.

New employees' references must be verified, and the employees must undertake to abide by the organization's Information Security policies.

All external suppliers who are contracted to supply services to the organization must agree to follow the Information Security policies of the organization. An appropriate summary of the Information Security Policies must be formally delivered to any such supplier, prior to any supply of services.

Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is classified as Proprietary (or above).

The organization's letter-headed notepaper, printed forms and other documents are to be handled securely to avoid misuse.

The lending of keys, both physical or electronic, is prohibited. This requirement is also to be noted in employment contracts.

Lending money to work colleagues is strongly discouraged.

All employees must comply with the Information Security Policies of the organization. Any Information Security 'incidents' resulting from non-compliance will result in immediate disciplinary action.

All employees to third party contractors are to sign a formal undertaking regarding the intellectual property rights of the work undertaken during their terms of employment/contract respectively.

All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after contractual relations with the organization.

***Confidential Personnel Data***

Notwithstanding the organization's respect for employee's privacy in the workplace, it reserves the right to have access to all information created and stored on the organization's systems.

***Handling Confidential Employee Information***

All employee data is to be treated as strictly confidential and made available to only properly authorized persons.

Only authorized personnel may give employee references.

All staff must have previous employment and other references carefully checked.

Employee data may only be released to persons specifically authorized to receive this information.

Employees are discouraged from sharing personal salary details and other terms and conditions with other members of staff.

***Personnel Information Security Responsibilities***



Employees may not use the organization's systems to access or download material from the Internet which is inappropriate, offensive, illegal, or which jeopardizes security. All Internet use must be for business related purposes.

All personnel must treat passwords as private and highly confidential. Non-compliance with this policy could result in disciplinary action.

Confidential information should be shared only with other authorized persons.

The use of e-mail for personal use is discouraged, and should be kept to a minimum. Postal mail may be used for business purposes only.

Personal calls on the telephone systems are to be minimized and limited to urgent or emergency use only.

The use of the organization's mobile phones will be monitored for inappropriate call patterns, unexpected costs, and excessive personal use.

'Company' Credit cards issued to authorized staff remain the responsibility of those employees until the card is returned or cancelled.

Only authorized employees may sign for the receipt of goods. They are to ensure that, by signing for them, they are not considered to be verifying the quality or condition of the goods.

Only properly authorized persons may sign for work done by third parties.

Only authorized persons may order goods on behalf of the organization. These goods must be ordered in strict accordance with the organization's purchasing policy.

All claims for payment must be properly verified for correctness before payment is effected.

Only authorized persons may approve expenditures or make commitments on behalf of the organization for future expenditures.

Telephone inquiries for sensitive or confidential information are initially to be referred to management. Only authorized persons may disclose information classified above Public, and then only persons whose identity and validity to receive such information has been confirmed.

All data and information not in the public domain, relating to the organization's business and its employees, must remain confidential at all times.

The playing of games on office PCs or laptops is prohibited.

Using the organization's computers for personal/private business is strongly discouraged.

### ***HR Management***

Management must respond quickly yet discreetly to indications of staff disaffection, liaising as necessary with Human Resources Management and the Information Security Officer.

Employee meeting and interview records must be formally recorded, with the contents classified as Highly Confidential and made available only to authorized persons.

### ***Staff Leaving Employment***

Upon notification of staff resignations, Human Resources Management must consider with the appointed Information Security Officer whether the member of staff's continued system access rights constitutes an unacceptable risk to the organization and, if so, revoke all access rights.



Departing staff are to be treated sensitively, particularly with regard to termination of their access privileges.

System and information access rights of employees who are transferring to competitors must be terminated immediately.

***HR Issues Other***

The organization does not encourage the recommending of professional advisors. References may, however, be given by authorized members of staff.



## *Chapter 10*

# CONTROLLING E-COMMERCE INFORMATION SECURITY

### *E-Commerce Issues*

E-commerce processing systems including the e-commerce Web site(s) are to be designed with protection from malicious attack given the highest priority.

E-commerce related Web site(s) and their associated systems are to be secured using a combination of technology to prevent and detect intrusion together with robust procedures using dual control, where manual interaction is required.

The organization's 'e-commerce' Web site(s) must be configured carefully by specialist technicians to ensure that the risk from malicious intrusion is not only minimized but that any data captured on the site, is further secured against unauthorized access using a combination of robust access controls and encryption of data.

Where third parties are involved in e-commerce systems and delivery channels, it is essential that they are able to meet the resilience and Information Security objectives of the organization.

## *Chapter 11*

### **DELIVERING TRAINING AND STAFF AWARENESS**

#### ***Awareness***

Permanent staff are to be provided with Information Security awareness tools to enhance the awareness and educate them regarding the range of threats and the appropriate safeguards.

An appropriate summary of the Information Security Policies must be formally delivered to any such contractor, prior to any supply of services.

An appropriate summary of the Information Security Policies must be formally delivered to, and accepted by, all temporary staff, prior to their starting any work for the organization.

The senior management of the organization will lead by example by ensuring that Information Security is given a high priority in all current and future business activities and initiatives.

The organization is committed to providing regular and relevant Information Security awareness communications to all staff by various means, such as electronic updates, briefings, newsletters, etc.

#### ***Training***

The organization is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise Information Security.

Periodic training for the Information Security Officer is to be prioritized to educate and train in the latest threats and Information Security techniques.

Individual training in Information Security is mandatory, with any technical training being appropriate to the responsibilities of the user's job function. When staff change jobs, their Information Security needs must be re-assessed and any new training provided as a priority.

Training in Information Security threats and safeguards is mandatory, with the extent of technical training to reflect the jobholder's individual responsibility for configuring and maintaining Information Security safeguards. When IT staff change jobs, their Information Security needs must be re-assessed and any new training provided as a priority.

All new staff are to receive mandatory Information Security awareness training as part of induction.

## *Chapter 12*

# DEALING WITH PREMISES RELATED CONSIDERATIONS

### ***Premises Security***

The sites chosen to locate computers and to store data must be suitably protected from physical intrusion, theft, fire, flood and other hazards.

Computer premises must be safeguarded against unlawful and unauthorized physical intrusion.

When locating computers and other hardware, suitable precautions are to be taken to guard against the environmental threats of fire, flood and excessive ambient temperature/humidity.

All computer premises must be protected from unauthorized access using an appropriate balance between simple ID cards to more complex technologies to identify, authenticate and monitor all access attempts.

All employees are to be aware of the need to challenge strangers on the organization's premises.

### ***Data Stores***

On-site locations where data is stored must provide 'access controls' and protection which reduce risk of loss or damage to an acceptable level.

Remote locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level.

### ***Other Premises Issues***

Electronic eavesdropping should be safeguarded against by using suitable detection mechanisms, which are to be deployed if and when justified by the periodic risk assessments of the organization.

The security of network cabling must be reviewed during any upgrades or changes to hardware or premises.

Owners of the organization's information systems must ensure that disaster recovery plans for their systems are developed, tested, and implemented.

## *Chapter 13*

### **DETECTING AND RESPONDING TO IS INCIDENTS**

#### ***Reporting Information Security Incidents***

All suspected Information Security incidents must be reported promptly to the appointed Information Security Officer.

Information Security incidents must be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This may only be done by authorized persons.

Any Information Security breaches must be reported without any delay to the appointed Information Security Officer to speed the identification of any damage caused, any restoration and repair to facilitate the gathering of any associated evidence.

All identified or suspected Information Security weaknesses are to be notified immediately to the Information Security Officer.

Persons witnessing Information Security incidents or breaches should report them to the Information Security Officer without delay.

Employees are expected to remain vigilant for possible fraudulent activities.

#### ***Investigating Information Security Incidents***

Information Security incidents must be properly investigated by suitably trained and qualified personnel.

Evidence relating to an Information Security breach must be properly collected and forwarded to the Information Security Officer.

Evidence relating to a suspected Information Security breach must be formerly recorded and processed.

The Information Security Officer must respond rapidly but calmly to all Information Security incidents, liaising and coordinating with colleagues to both gather information and offer advice.

#### ***Corrective Activity***

A database of Information Security threats and 'remedies' should be created and maintained. The database should be studied regularly with the anecdotal evidence used to help reduce the risk of frequency of Information Security incidents in the organization.

#### ***Other Information Security Incident Issues***

The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations.

Information Security incidents arising from system failures are to be investigated by competent technicians.

Breaches of confidentiality must be reported to the Information Security Officer as soon as possible.

During the investigation of Information Security incidents, 'dual control' and the 'segregation of duties' are to be included in procedures to strengthen the integrity of the information and data.

Staff shall be supported by management in any reasonable request for assistance together with practical tools, such as security incident check lists, etc., in order to respond effectively to an 'Information Security incident'.



Where a risk assessment has identified an abnormal high risk from the threat of electronic eavesdropping and/or espionage activities, all employees will be alerted and reminded of the specific threats and the specific safeguards to be employed.

Information relating to Information Security incidents may only be released by authorized persons.



## Chapter 14

### CLASSIFYING INFORMATION AND DATA

#### *Setting Classification Standards*

The organization must record, maintain and update a data base of its 'information assets'.

All information, data and documents are to be clearly labeled so that all users are aware of the ownership and 'classification' of the information.

All information, data and documents must be processed and stored strictly in accordance with the 'classification' levels assigned to that information.

All information, data or documents 'classified' as highly sensitive (Top Secret) must be stored in a separate secure area.

All information, data or documents must be 'classified' according to their level of confidentiality, sensitivity, value and criticality.

All information, data and documents are to be the responsibility of a designated information owner or custodian.

Access to the resources available from the organization's network must be strictly controlled in accordance with the agreed 'Access Control List', which must be maintained and updated regularly