

Company Name

Date

1.1 – Information Security Policy

An Information Security Policy sets your company's requirements, direction and management support for information security.

	Yes	Partially	No
Does your organisation have an information security policy?			
If yes, please answer the following:			
Has this policy been agreed by senior management?			
Do you make staff aware of this policy? E.g. at their induction?			
Can staff access this policy at any time? E.g. via an Intranet.			
Is adherence to this policy included in staff contracts?			
Is someone responsible for the maintenance of the policy?			

2.1 – Information Security Infrastructure

An Information Security Infrastructure is a crucial element of an overall security plan, which if effectively deployed, ensures that Information Security is implemented and managed within your company.

	Yes	Partially	No
Has your organisation implemented an information security infrastructure?			
If yes, please answer the following:-			
Does a director (or equivalent) have responsibility for information security?			
Have designated staff been given specific security responsibilities as part of their existing duties, e.g. IT Manager?			
Is information security represented as an agenda item at regular senior management meetings?			
Is expertise on Information Security available internally, and where not, is external advice sought when required?			

2.2 – Third Party Access

The security of your company's information, if accessed by third parties, must be ensured.

	Yes	Partially	No
Is third party access to information managed within your organisation?			
If yes, please answer the following:			
If a third party, e.g. a Joint Venture, has access to information, does this access require approval by an appropriate manager?			
If access is allowed, are the associated risks assessed and the appropriate security measures put in place?			
Do third party contracts address information security matters, such as liabilities, data protection, intellectual property and copyright?			

2.3 – Outsourcing

The security of information needs to be maintained when the responsibility for information processing has been outsourced to another organisation, e.g. use of an ISP.

	Yes	Partially	No
Does your organisation outsource IT?			
If yes, please answer the following:			
Are security requirements explicitly stated or formally agreed between parties?			
Are security requirements addressed in the contract between your organisation and the other party?			

3.1 – Asset Classification & Control

The maintenance of assets can be greatly enhanced through the use of an inventory.

	Yes	Partially	No
Does your company maintain an inventory of assets?			
If yes, please answer the following:			
Do you maintain an inventory of information assets, e.g. databases?			

	Yes	Partially	No
Do you maintain an inventory of software assets?			
Do you maintain an inventory of hardware assets?			
Do you maintain an inventory of services, such as utilities?			

3.2 – Information Classification

Information has varying degrees of sensitivity and criticality. By classifying information, the appropriate level of protection can be specified.

	Yes	Partially	No
Does your company classify information?			
If yes, please answer the following:			
Are information classification guidelines in operation?			
Do you tell staff how they should handle information with regard to its storage, postage and destruction?			
Is the responsibility for classifying information clearly defined?			
Are staff required to lock away sensitive documents when not in use?			

4.1 – Personnel Security

Security responsibilities should be addressed in contracts and should be monitored during employment.

	Yes	Partially	No
Are specific personnel measures taken with respect to security?			
If yes, please answer the following:			
Are staff aware of their security responsibilities via details in their job descriptions?			
Are job applicants' claims of previous experience, qualifications and identity, and character references verified?			
Are employees and contract staff required to sign confidentiality or non-disclosure agreements?			

4.2 – User Training

User training is crucial to ensuring that staff are adequately equipped to support the security policy in the course of their normal work.

	Yes	Partially	No
Is information security training provided?			
If yes, please answer the following:			
Do all staff receive basic information security training at induction e.g. use of passwords?			
Is the training provided periodically? E.g. monthly, yearly			
Do staff with specific responsibilities (e.g. IT Manager) receive additional training?			

4.3 – Responding to Security Incidents and Malfunctions

To minimise the damage from security incidents, and to monitor and learn from such incidents, they should be reported and managed as quickly as possible.

	Yes	Partially	No
Does your organisation respond to security incidents?			
If yes, please answer the following:			
Are staff and contractors made aware of how to recognise and report security incidents, suspected weaknesses or threats to systems?			
Is someone responsible for reviewing and progressing the closure of reported incidents?			
Are employees who violate the security policy subject to a disciplinary process?			

5.1 – Secure Areas

It is important that measures are taken to prevent unauthorised access, damage and interference to business premises and information processing facilities.

	Yes	Partially	No
Does your organisation take steps to prevent unauthorised access to your premises?			
If yes, please answer the following:			
Does each entrance have some form of physical access control?			

	Yes	Partially	No
Are secure areas (such as computer rooms) or office areas where sensitive information is stored, protected by access controls?			
Are visitors always signed in and escorted around the building?			
Are unmanned external doors and accessible windows protected through additional controls?			

5.2 – Equipment Security

Equipment should be protected against security threats and environmental hazards.

	Yes	Partially	No
Does your organisation take steps to prevent loss, damage or compromise of equipment and interruption to business activities?			
If yes, please answer the following:			
Is important equipment, e.g. servers, located in secure areas?			
Is equipment protected from power failure, e.g. use of a UPS?			
Is equipment maintained in accordance with the manufacturer's requirements?			
Is guidance provided with regard to the use of company material off-site, e.g. use of a laptop?			

5.3 – General Controls

General controls are required to prevent compromise or theft of information.

	Yes	Partially	No
Does your organisation implement general measures to protect the company's information?			
If yes, please answer the following:			
Is there a "clear desk" policy in operation?			
Are paper and computer media locked away when not in use?			
Are computers left logged on whilst unattended?			

6.1 – Operational Procedures & Responsibilities

Operational procedures and responsibilities are required to ensure the correct and secure operation of information systems.

	Yes	Partially	No
Do you have effective, formal operational procedures?			
If yes, please answer the following:			
Are key tasks for computer systems, such as back-up and restoration, documented?			
Are changes to systems, e.g. installing a new piece of software, justified and managed?			
Do you have incident management procedures covering areas such as system failures, viruses and breaches of confidentiality?			
Are job roles (where practical) segregated to help prevent incidents such as fraud?			

6.2 – Systems Planning & Acceptance

The risk of system failures should be minimised by system planning and acceptance.

	Yes	Partially	No
Are methods used to plan and accept systems?			
If yes, please answer the following:			
Is capacity on systems monitored, and future capacity projected?			

6.3 – Protection Against Malicious Software

Are precautions taken against the introduction of malicious software such as viruses and worms?

	Yes	Partially	No
Are formal anti-virus measures in operation?			
If yes, please answer the following:			
Do you have an anti-virus policy?			
Is anti-virus software operating on all servers, PCs and mobile computers?			
Are anti-virus updates rigorously applied?			

6.4 – Housekeeping

Housekeeping helps maintain the integrity and availability of information and communication systems through the deployment of techniques such as information back-up.

	Yes	Partially	No
Are back-up procedures documented and in place?			
If yes, please answer the following:			
Have procedures been established covering data back-up and recovery?			
Is back-up data stored off-site in a secure manner?			
Are procedures for the recovery of data regularly tested?			
Are logs maintained as to who has made the back-up and when?			

6.5 – Network Management

The information in networks must be safeguarded, and supporting infrastructure protected.

	Yes	Partially	No
Is your company's network connected to public networks?			
If yes, please answer the following:			
Are controls, where required, used to conceal the meaning of text, e.g. cryptography?			
Have controls been implemented to protect systems connected to the internet, e.g. firewalls?			

6.6 – Exchanges of Information & Software

The exchange of information between organisations must be protected against loss, modification or misuse.

	Yes	Partially	No
Are protective measures in place to ensure the security of e-commerce services provided to trading partners or the public?			

	Yes	Partially	No
If yes, please answer the following:			
If you trade over the internet do you ensure this trade is covered by terms and conditions before the trade commences?			
Is e-commerce data protected from disclosure or modification, e.g. use of cryptography?			
Are appropriate mechanisms used to authenticate users, e.g. Log on & Password?			
Is the integrity of publicly available data appropriately assured e.g. does the individual responsible for drawing up a price list for its accuracy?			
Do you have a policy on the use of e-mail?			

7.1 – Business Requirements for Access Control

Access to information should be controlled on the basis of both business and security requirements.

	Yes	Partially	No
Does your company control access to information?			
If yes, please answer the following:			
Do you have an access control policy, e.g. defining who has access to what information?			
Is access granted on a "need to know" basis?			

7.2 – User Access Management

Good user access management helps ensure that unauthorised access to information systems is prevented.

	Yes	Partially	No
Does your company have user access management procedures in place?			
If yes, please answer the following:			
Is there a formal registration process before access is permitted?			
Are access requests and authorisations documented and retained?			
Are unique user IDs deployed so that users can be held accountable?			

	Yes	Partially	No
Do you maintain records of all staff given access to the system?			
Are access rights immediately removed when a user leaves?			
Do you undertake a periodic review of user access rights?			
Is access given only to authorised members of staff?			
Are records of all privileges issued to staff retained?			
Is the allocation of passwords endorsed through a formal process?			
Must users change the password allocated when they first log-on?			

7.3 – User Responsibilities

The prevention of unauthorised user access is dependent upon user responsibility as well as technical access control.

	Yes	Partially	No
Are users given guidance on their responsibilities for access control?			
If yes, please answer the following:			
Do you issue documented guidelines on the selection and use of passwords?			
Can users change their password at any time, for example if they suspect that it has been disclosed?			
Is there a minimum password length?			
Are terminal time-outs enforced?			

7.4 – Operating System Access Control

Security facilities at the operating system level should be used to restrict access to computer resources.

	Yes	Partially	No
Are users restricted from sharing user IDs?			

	Yes	Partially	No
If yes, please answer the following:			
Is the number of consecutive unsuccessful log-on attempts restricted?			
Do default passwords need to be changed prior to use in the live environment?			

7.5 – Application Access Control

Some organisations use applications for their day to day working and these applications become critical to overall operation. It is crucial that these applications are protected.

	Yes	Partially	No
Do you use an application that is crucial to the operation of company?			
If yes, please answer the following:			
Does the application allow restriction of access, e.g. password protection?			
Is restriction of the application enforced through an access control policy?			

7.6 – Mobile Computing & Teleworking

Information security must be ensured when using mobile computing and teleworking facilities.

	Yes	Partially	No
Do you have any mobile computing, teleworking facilities?			
If yes, please answer the following:			
Do restrictions apply to mobile computing, teleworking facilities?			
Does your security policy or guideline address the use of mobile computing facilities and teleworking?			
Is teleworking authorised and controlled by management?			
Is teleworking monitored and access usage reviewed?			

8.1 – Security Requirements of Systems

This section is concerned with the internal development of applications that will subsequently be used for the operation of a company.

	Yes	Partially	No
Do you develop applications internally?			
If yes, please answer the following:			
Are security requirements determined following a risk assessment of the proposed system?			
Is the Project Manager assigned responsibility to include the requirements of information security?			
If cryptographic controls are used is there a documented policy on their deployment and use?			
Are industry standard cryptographic controls used?			
Is test data protected and controlled?			
Is strict access maintained over programme source libraries?			
Are formal change control procedures used to enforce and govern how programmes are moved from development into production?			
Are application systems tested whenever changes to the operating systems are made?			

8.2 – If No to 8.1.....

	Yes	Partially	No
Do you use outside contractors for development activity?			
If yes, please answer the following:			
Do you ensure formal agreements exist that stipulate that contractors must comply with good practice?			
When development is outsourced, do you ensure you have the right to audit?			

9.1 – Aspects of Business Continuity Management

Critical business processes need to be protected from the effects of major failures or disasters.

	Yes	Partially	No
Do you have any Business Continuity Plans?			
If yes, please answer the following:			
Is a nominated individual responsible for managing the Business Continuity process?			
Is a Business Impact Analysis carried out to identify the events that can cause interruptions?			
Is there a regular programme of Business Continuity Process testing?			

10.1 – Compliance with Legal Requirements

The design, operation, use and management of information systems should comply with all relevant criminal and civil law, statutory, regulatory or contractual obligations.

	Yes	Partially	No
Do you ensure that you meet any legal requirements / obligations?			
If yes, please answer the following:			
Is (are) a nominated individual(s) responsible for maintaining knowledge of all applicable legislation, including copyright and data protection?			
Can you demonstrate that you adhere to licensing agreements?			
Are guidelines available for the safeguarding and retention periods of important organisational records such as accounting records?			
Do you make users aware of the Computer Misuse Act?			

10.2 – Review of Security Policy & Technical Compliance

The security of information systems should be regularly reviewed to ensure on-going compliance of systems with organisational security policies and standards.

	Yes	Partially	No
Do you undertake any review of your information systems with regard to legal compliance?			
If yes, please answer the following:			
Do you regularly check your information systems for compliance with security standards, e.g. through an internal audit programme?			
Are the results of internal audits and reviews used to manage information security?			
Is penetration testing of firewalls regularly carried out?			

10.3 – Systems Audit Considerations

The effectiveness of the system audit process should be maximised and interference with the audit process minimised.

	Yes	Partially	No
Are system audits undertaken?			
If yes, please answer the following:			
Are audit plans and scope agreed prior to the audit?			