Computer and information security standards
Computer and information security standards
Computer and information security standards

Disclaimer

The Computer and Information Security Standards and accompanying CISS Workbook (each a publication) is © The Royal Australian College of General Practitioners ABN 34 000 223 807. The information set out in each publication is current at the date of first publication and is intended for use as a guide of a general nature only and may or may not be relevant to particular patients or circumstances. Nor is each publication exhaustive of the subject matter. Persons implementing any recommendations contained in the publications must exercise their own independent skill or judgment or seek appropriate professional advice relevant to their own particular circumstances when so doing. Compliance with any recommendations cannot of itself guarantee discharge of the duty of care owed to patients and others coming into contact with the health professional and the premises from which the health professional operates.

Whilst the text is directed to health professionals possessing appropriate qualifications and skills in ascertaining and discharging their professional (including legal) duties, it is not to be regarded as definitive professional advice and, in particular, is no substitute for a full consideration of particular circumstances and requirements of the user based on accepted practices.

Accordingly The Royal Australian College of General Practitioners and its employees and agents shall have no liability (including without limitation liability by reason of negligence) to any users of the information contained in these publications for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of any person using or relying on the information contained in these publications and whether caused by reason of any error, negligent act, omission or misrepresentation in the information.
Acknowledgments

The RACGP Computer and Information Security Standards (CISS) and the accompanying CISS Workbook is a major revision of the Standards for computer security: a self assessment guide and checklist for general practice (3rd edition) which was based on the Computer security self-assessment guideline and checklist for general practitioners (2nd edition) published in 2005 by the General Practice Computing Group, and on work done in 2001 by The Royal Australian College of General Practitioners and the Australian Medical Association.

The Royal Australian College of General Practitioners gratefully acknowledges the following people who were involved in the development, review and writing of CISS:

- Dr Patricia A H Williams PhD (Security Research Centre, Edith Cowan University, Perth, WA)
- Dr John W Bennett PhD (Chair of RACGP National Standing Committee for e-health)
- RACGP National Standing Committee for e-health
- Judy Evans, Manager e-health, RACGP
- Angela Whitworth, Project Officer, RACGP
Contents

Preface 6

1 Introduction 10
  1.1 How to use this document 10

2 Computer and information security checklist 11

3 Organisational and technical issues 13
  3.1 Risk assessment 13
    3.1.1 Select security coordinator 14
    3.1.2 Articulate the operating parameters 14
    3.1.3 Record all user and technical support contact details 15
    3.1.4 Asset register 15
    3.1.5 Identify the threats and vulnerabilities, and suggested controls 15
    3.1.6 Identify appropriate controls 16
    3.1.7 Security management and reporting, including monitoring compliance and review planning 16
    3.1.8 Education and communication 16
    3.1.9 Breach reporting 16
  3.2 Staff roles and responsibilities 18
    3.2.1 Practice computer security coordinator 19
    3.2.2 Other staff roles and responsibilities 20
  3.3 Practice security policies and procedures 21
    3.3.1 Practice security policies and procedures description 22
    3.3.2 Sample confidentiality agreement 24
    3.3.3 Contractual agreements 26
  3.4 Access control and management 27
    3.4.1 Setting access levels 29
    3.4.2 Access policy 29
  3.5 Business continuity and disaster recovery plans 31
    3.5.1 Business continuity and disaster recovery 33
    3.5.2 Development process and procedures 34
  3.6 Staff internet and email usage 38
    3.6.1 Policies for the use of internet and email 39
    3.6.2 Procedures for the safe use of internet and email 40
  3.7 Backup 42
    3.7.1 Backup procedure 44
    3.7.2 Backup media cycling 44
    3.7.3 Documenting rotation of backup media 45
    3.7.4 Restoring data 45
## Contents

3.8 Malware, viruses and email threats 46

3.8.1 Malware and virus protection 47

3.9 Network perimeter controls 48

3.9.1 Network perimeter control policy 49

3.9.2 Intrusion detection system 49

3.9.3 Firewall 49

3.9.4 Other controls 49

3.10 Portable devices and wireless networks 50

3.10.1 Portable devices 51

3.10.2 Remote access 51

3.11 Physical, system and software protection 52

3.11.1 Physical 55

3.11.2 System maintenance 56

3.11.3 Software maintenance 56

3.12 Secure electronic communication 57

3.12.1 Healthcare identifiers 59

3.12.2 Message system record 59

4 Conclusion 60

Glossary of computer and information security terms 61
Preface

The use of clinical desktop systems and the electronic management of information has become a vital tool in the delivery of safe and high quality care for patients. Many practices use a combination of the skills of their staff and the engagement of external information technology (IT) consultants to install and maintain their computer systems and security. General practice has specific requirements in computer and information security and it can be a challenge to find external security experts and technical service providers who understand the business of delivering care in the general practice environment. In essence, general practices need to put in place good information management and security processes. This will include aspects such as governance processes, understanding the risks to information, good planning and implementing appropriate security measures.

The important aspects of computer and information security for general practices include:

• Information management processes. Managing the use of information, its ongoing availability and the processes associated with this, need effective administration. This includes fundamental information security processes such as:
  – Backup procedures that are documented and tested. It is important to ensure that the backup system functions correctly and that data can be recovered if there is an incident such as a server failure.
  – Business continuity and disaster recovery planning. Documented business continuity plans that include disaster recovery procedures are essential to maintaining information availability so that in the event of a ‘disaster’ there is an adequately planned response, and potential loss or corruption of information is minimised. These plans also detail how to maintain the critical functions in the event of an incident.
  – Access control and management. Control of who has access to practice information is essential to the protection of all practice data. Access management (password and/or biometrics) allows accountability; without this it can be difficult to ascertain who has entered or altered data, including clinical records. Without these controls the practice is vulnerable to unauthorised information access.

• Risk analysis. It is important to understand the security risks and threats to practice information. This includes the requirement for effective information security practices by identifying gaps in security and using strategies to lessen these security risks. Ensuring that information held on practice computer systems is secure is essential to the running of a general practice, to maintaining professional responsibilities to patients, and to ensure that practice information is accurate and available when it is needed.

• Good governance. It is important to have sound information security governance in place to ensure that all computer and information security processes are documented and followed. To enable this, responsibility should be allocated to one person to oversee this for the practice. This person
should coordinate security related activities and assist in identifying the need for external technical service providers and when it is appropriate to engage their services. Computer and information security requires regular attention at a practice level and all staff need to be aware of their responsibility in protecting practice information. Monitoring and reporting also form part of this governance process.

- Developing a security ‘culture’ and demonstrated leadership. It is important that one or more people within the practice take responsibility for computer and information security. It is also beneficial to promote a culture of security within the practice. This includes educating staff about the risks to the practice information systems and the maintenance of practical policies that direct staff in their management of the security risks.

The RACGP Computer and Information Security Standards and accompanying Workbook detail the knowledge needed by practice staff, the basic security processes that are required, and indicate when it may be necessary to engage technical IT and security expertise.

The CISS takes into account the increased use of laptops, remote access devices (such as personal digital assistants [PDA], iPads, USB flash drives, and removable hard drives) and wireless (Wi-Fi) connections. Additionally, it prepares the practice for a connected e-health environment. The practice server and network now assumes an increasingly vital role in practice management with clinical and practice management software becoming more complex. Additionally, there is widespread uptake of broadband internet and secure messaging, particularly in the implementation of the e-health initiatives such as the Department of Health and Ageing’s personally controlled electronic health record (PCEHR). Healthcare Identifiers which are explained in detail in section 3.12, are key to many of these initiatives.

Note: The security standards do not address patient access to medical records or the management of pathology and/or radiology results. Staff need to be aware of the 4th edition RACGP Standards for general practices that detail the overarching professional standards related to patient access to information and the associated security and privacy issues. The principal aim of these standards is to highlight the processes, policies and procedures that will protect your practice’s information.

It is a challenge to produce a standard that will suit all practices. The computer system requirements of large practices differ from those of solo practices; practices vary in their level of staff computer skills; ‘paperless’ practices will have different needs to those using a hybrid system; and rural practices may have less access to technical support. It is therefore important for all practices to apply a risk analysis of their particular systems and security needs, and to document the policies and procedures that staff will need to adhere to, so that
there is an assurance of availability, integrity and confidentiality of all information held within the practice’s clinical and administrative systems.

These standards have been formulated to meet achievable best practice in computer and information security. They have been developed in alignment with international and Australian standards below, and have been informed by advice from security experts.

- **AZ/NZS ISO 31000:2009 Risk management – principles and guidelines.**
  Sydney: Standards Australia International, 2009
- **HB 292 – 2006 A practitioners guide to business continuity management.**
  Sydney: Standards Australia International, 2006
- **HB 174 – 2003 Information security management – implementation guide for the health sector.**
  Sydney: Standards Australia International, 2003. Note: this handbook is due for revision shortly
- **HB 231 – 2004 Information security risk management guidelines.**
  Sydney: Standards Australia International, 2004
- **HB 292 – 2006 A practitioners guide to business continuity management.**
  Sydney: Standards Australia International, 2006
- **HB 293 – 2006 Executive guide to business continuity management.**
  Sydney: Standards Australia International, 2006
- **Information Privacy Principles under the Privacy Act 1988**
These standards are also designed to meet international standards in health information security specifically:

**National Privacy Principles**

**Principle 4 – Data security**

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

**Australian Information Privacy Principles**

**Principle 4 – Storage and security of personal information**

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected by, such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.
1 Introduction

Maintaining effective computer and information security in general practice is vital and requires planning and technical knowledge. This standards document is a practical guide for Australian general practice. It provides an optimal set of controls and procedures for implementing and maintaining computer and information security within the capabilities of most Australian general practices. It is not a technical manual, but will assist practices to understand what is needed in order to put in place optimum computer and information security strategies.

When reading these standards, bear in mind that it is about computer and information security and refers to:
- confidentiality of information – only authorised people can access the information
- integrity of information – only authorised people can alter the information
- availability of information – available and accessible when needed.

There are differences between privacy and confidentiality. In the health context, privacy is concerned with a person, whilst confidentiality is about information and how it is managed. Privacy relates to an individual's control over the use, disclosure and sharing of information collected about them. Confidentiality relates to the processes put in place to handle information once it has been disclosed; such as how it is stored, access control procedures, encryption of data and how it is shared.

1.1 How to use this document

There are three parts to this document suite:

1. A checklist which will determine whether you have established reasonable computer security measures in your practice to protect the information the practice holds.

2. An explanation and advice section for each computer and information security concern that your practice will have to address. Each section assists you to understand and put in place the correct security procedures. It includes an explanation and potential impact of security concerns. This includes why practices should spend time and money on protection from the risks and the potential impact this may have. It also includes the actions that will minimise any potential impact on the protection of the information. This lists the processes and procedures that should be put in place to manage any risks to the information.

3. A supporting CISS Workbook containing examples, tables and forms to assist in developing and recording policies and procedures for computer and information security. This document can be downloaded from the RACGP website (www.racgp.org.au/ehealth). By adding information that is relevant to your practice, you can incorporate this workbook directly into your practice’s policies and procedures manual.
## 2 Computer and information security checklist

This checklist provides a record of the 12 basic computer and information security categories that should be undertaken. The checklist is a guide only and does not describe the complete list of security activities that should be undertaken. Details of these are provided in the subsequent document sections. This checklist can also be found in the CISS Workbook, section 1.

<table>
<thead>
<tr>
<th>Category</th>
<th>Tasks</th>
<th>Completed (Tick and date)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Risk assessment</td>
<td>Conduct risk assessment activities and put procedures in place</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td>2. Staff roles and responsibilities</td>
<td>Practice computer security coordinator’s roles documented</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Select practice staff member(s) for security coordinator role</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Computer security training for coordinator(s) provided</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td>3. Practice security policies and procedures</td>
<td>Computer and information security policies documented</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Computer and information security procedures developed</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Staff trained in computer security policies and procedures</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Individual staff agreements for confidentiality and computer use signed</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td>4. Access control and management</td>
<td>Staff policy developed on levels of access to data and information systems</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Staff assigned appropriate access level</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Staff have individual passwords that are changed on a regular basis</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Confidentiality agreements for third party providers in place</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td>5. Business continuity and disaster recovery plans</td>
<td>Business continuity plan completed</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Disaster recovery plan completed</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Business continuity and disaster recovery plans tested</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Business continuity and disaster recovery plans reviewed and updated</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td>6. Staff internet and email usage</td>
<td>Staff trained in appropriate use of internet and email</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td>7. Backup</td>
<td>Backup of data done daily, with weekly, monthly and yearly copies retained</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Backups encrypted</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Backup of data stored securely on and off site</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Backup procedure tested by performing a restoration of data</td>
<td>__ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Backup procedure included in the documented business continuity and disaster recovery plans</td>
<td>__ / __ / __</td>
</tr>
</tbody>
</table>
### Computer and information security checklist

**Date of assessment: ___ / ___ / ___**

<table>
<thead>
<tr>
<th>Category</th>
<th>Tasks</th>
<th>Completed (Tick and date)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. Malware, viruses and email threats</td>
<td>Antivirus and antimalware software installed on all computers</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Automatic updating of virus definitions is enabled on all computers/server</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Staff trained in antimalware procedures</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Automatic weekly scans are enabled</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td>9. Network perimeter controls</td>
<td>Hardware and/or software network perimeter controls installed</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Hardware and/or software network perimeter controls tested periodically</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Intrusion activity logs monitored and breaches reported</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td>10. Portable devices and wireless networks</td>
<td>Portable devices (memory devices, backup media) are kept secure</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Wireless networks configured securely</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Policy on the use of mobile devices developed</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Remote access protection in place (eg. virtual private networks (VPN)</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td>11. Physical, system and software protection</td>
<td>Physical security of the server and network maintained</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Uninterruptible power supply and surge protectors installed</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Staff aware of appropriate confidentiality of information (eg. clear screen and clear desk procedures)</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Preventative system maintenance undertaken regularly</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Software updates and patches applied as soon as they become available</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td>12. Secure electronic communication</td>
<td>Secure messaging system (involving encryption) used for the electronic transfer of confidential information</td>
<td>❌ __ / __ / __</td>
</tr>
<tr>
<td></td>
<td>Safe and secure use of email, internet and the practice website policy developed and reviewed periodically</td>
<td>❌ __ / __ / __</td>
</tr>
</tbody>
</table>
3 Organisational and technical issues

3.1 Risk assessment

Regardless of the size of the general practice, it is imperative that there is an understanding and analysis of the threats and vulnerabilities that practices are open to, and the risk that these pose to the computer and information systems. This allows the selection of the most appropriate security controls to be put in place to minimise these risks. Therefore the first task in ensuring effective information security is to undertake a risk assessment.

The method suggested in this standard has been adapted from established risk assessment and management processes and simplified to make it as practical and straightforward as possible for practices to undertake themselves. The entire risk management process involves establishing the context, identifying the risks, analysing the risks, evaluating the risks and treating the risks.

There are elements that require time to document, such as the asset register, however this information is subsequently reused in the business continuity and disaster recovery plans. Avoidance of this activity will mean that a practice does not have a strong foundation for their computer and information security choices and may not have effective protection of the practice information. In addition, documentation of risk assessment also provides evidence of a proper and systematic approach to security and demonstrates defensible governance. Records should be retained on physical and information assets. As an ongoing practice, each breach in security (accidental or intentional) should be recorded.

Actions

Below is a list of activities that make up a risk assessment. The tables for filling in this information can be found in the CISS Workbook section 2.

- Select practice staff member who will take on the security coordination role (refer to section 3.2 for role responsibilities).
- Articulate the operating parameters (i.e. legal and professional information use and protection requirements) see section 2.2 of the CISS Workbook.
- Record the role in the practice and contact details for all users and those who may potentially have access to the information systems. This includes internal full time, locum and casual staff, clinical and non-clinical, external third party and technical service providers, and support staff such as cleaners.
- Identify and record details of all computer and information assets. This is more commonly known as an asset register. The CISS Workbook provides a detailed list of the most common assets and what information needs to be recorded about these assets. This includes physical equipment, software and information assets.
Identify the threats to and vulnerabilities of the assets that could adversely affect practice operations and match suitable controls to these. Note: In traditional risk assessment methodologies this task is quite detailed and is divided into identifying threats and vulnerabilities and then deciding on the likelihood and impact to give a risk level. To ensure that the risk assessment process is achievable for general practice this step has been pre-determined and examples of the threats and vulnerabilities provided in Table 22 of the CISS Workbook, section 2.5.

Identify current and proposed controls to minimise the risk and develop an action plan around these.

Security management and reporting including monitoring and review planning.

Ongoing education and communication. Security is both a technical and social activity, and staff are a good source of information about risks and feedback on security controls and their effectiveness. Keeping staff up to date and aware of potential risks is vitally important to the ongoing protection of your computer and information security.

Breach recording.

Refer to the CISS Workbook, section 2 for the risk assessment process.

3.1.1 Select security coordinator
Select the person or persons in the practice team who will undertake the coordination of computer and information security in the practice. Refer to section 3.2 of this document for a definition of the role and responsibilities of the computer security coordinator.

3.1.2 Articulate the operating parameters
The practice should be able to answer the questions below in regard to the legal and professional parameters of the practice environment. To ensure that all staff understand the specific requirements of computer and information security as they apply to the setting in which they work, it is important to document these answers.

- What are the legal and professional requirements for the protection of the information for which the practice is custodian?
- What capabilities does the practice have in terms of security knowledge and expertise?
- Who makes the decisions about the security protections to be put in place?
- What processes are in place to assist in decision making regarding the use of the information the practice holds? For example, in the instances of secondary use of data or freedom of information requests.

Refer to CISS Workbook, section 2.2 for examples and to record this information.
3.1.3 Record all user and technical support contact details

Record all users and those who may potentially have access to the information systems (refer to CISS Workbook, section 2.3). This includes internal full time, locum and casual staff, clinical and non-clinical, external third party and technical service providers and support staff (such as cleaners). This should be kept up to date as staff leave the practice and new staff commence.

3.1.4 Asset register

Developing an asset register may require assistance from your technical service provider. The asset register documents the computer hardware, software and information belonging to the practice or under the custodianship of the practice, and where it is used and stored. The register also records the configuration of the system which will be used when the business continuity or disaster recovery plan is invoked. The asset register must be updated as each new item is purchased by the practice or new service or application installed. The computer security coordinator should maintain the asset register.

Refer to CISS Workbook, section 2.4 for examples and to record this information. The assets are grouped as follows:

- Physical assets – computer and communications equipment, backup media, power supplies and furniture. Diagrams showing the layout of the network and computers are a useful resource to include.
- Electronic information assets – databases, electronic files and documents, image and voice files, system and user documentation, business continuity and disaster recovery plans.
- Software assets – application programs, operating system, communications software. Include all clinical and practice management software, as well as email, firewall, backup, virus checking and other utilities. Original software media and manuals should be stored securely.
- Personnel assets – staff and contractors. Contact details of all staff are contained in Table 1 of the CISS Workbook, section 2.3.
- Paper documents – contracts, operating and professional guidelines.

3.1.5 Identify the threats and vulnerabilities, and suggested controls

This activity aims to minimise the impact from potential threats and vulnerabilities that could adversely affect the practice. This includes financial loss, breaches in confidentiality, information integrity and availability, and patient confidence. Table 22 in the CISS Workbook, section 2.5 has been formulated with the common threats and vulnerabilities that face a general practice, and suggested controls to minimise the risks and impact of these.

Identify the threats, potential hazards and vulnerabilities to the information assets that could adversely affect practice operations. The threats have been categorised into three areas:

- human (unintentional and deliberate)
- technical
- environmental.
3.1.6 Identify appropriate controls
The purpose of selecting appropriate controls is to reduce the risk or reduce the adverse consequences following an incident. Once the threats and vulnerabilities have been identified, the existing controls implemented in the practice need to be added to Table 22 in the CISS Workbook, section 2.5. Following this step, the existing controls should be compared to those suggested and any additional required controls (actions to take) should be added to the table. This will form part of your plans for improving the security of your practice computer and information systems. This is referred to as a gap analysis.

To decide the actions to take, consideration must be given to the cost-effectiveness of controls for your practice in order to minimise the risks. Control selection will be based on cost, ease of use, integration with normal workflow, importance to practice, and objective of protection. Selection of controls is also impacted by the financial and time constraints of the practice, as well as the technical and legal skill of staff.

Note: There will always be a residual risk after the implementation of security controls. This is unavoidable and no system can ever be absolutely secure. In addition, some level of risk acceptance may be intentional because of low possibility of occurrence and the high cost to protect against the risk. It is important to be aware of these risks that have a level of acceptance.

3.1.7 Security management and reporting, including monitoring compliance and review planning
Document the planned monitoring for compliance to statutory obligations and review period for the risk assessment process. This is particularly important when computer equipment and software are updated, new uses of information are embarked on (such as health information exchange, the Personally Controlled Electronic Health Record (PCEHR) and secondary use of information), staff leave or new staff commence, when changes occur to legislation or professional requirements, or following incidents or breaches in information security.

3.1.8 Education and communication
Effective communication and education of all staff about the risks that the practice computer and information are open to, is an important aspect of risk management. Discussion at practice meetings and being part of governance processes of the practice are essential.

3.1.9 Breach reporting
The practice policy will document the procedures on the detection and reporting of breaches of security. This policy will also incorporate identified ongoing training needs of staff, reporting procedures and consequences for noncompliance with the policy.
The following form could be used to report all incidents both accidental and intentional. This form can also be found in the CISS Workbook, section 2.9.

<table>
<thead>
<tr>
<th>Practice name</th>
<th>Incident – breach report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report date/time:</td>
<td></td>
</tr>
<tr>
<td>Author:</td>
<td></td>
</tr>
<tr>
<td>Details of the incident (date, time, what happened, impact and information system affected):</td>
<td></td>
</tr>
<tr>
<td>Actions taken (who contacted, corrective action taken):</td>
<td></td>
</tr>
<tr>
<td>Outcome:</td>
<td></td>
</tr>
<tr>
<td>Future actions required (eg. ensure malware protection up to date):</td>
<td></td>
</tr>
</tbody>
</table>
3.2 Staff roles and responsibilities

The practice computer security coordinator draws together the computer and information security issues that confront the practice – this is a leadership role. The coordinator manages the training and is responsible for maintaining staff knowledge of computer and information security principles and practice security policy and procedures. The role also includes managing the risk assessment, creation and policy review, and the security management and reporting functions. The practice security coordinator might be one of the doctors, a nurse, a senior receptionist or the practice manager. These tasks can be allocated to more than one person in the practice.

The coordinator’s role is primarily to raise computer security awareness rather than being a technical ‘fix-it’ person. They should help to create interest, even enthusiasm, for an IT security ‘culture’ and ensure that there is adequate and appropriate training for all staff. They also need to understand that while many aspects of computer and information security are outsourced to technical service providers, certain responsibilities and tasks need to be carried out by practice staff, e.g. checking the backup procedure. While many practices now outsource aspects of computer maintenance to technical service providers, a practice computer security coordinator needs to be aware of what needs to be done, even though they may not have the technical knowledge to do these tasks themselves. A generic role description for the computer security coordinator is given in section 3.2.1.

All practice staff should be aware of their responsibility in regards to information security. While the role for coordinator is well defined, it should be made explicit in the practice policies what role and responsibility each member of the practice must assume in the protection of information. Staff awareness of their role in information security is vital. This includes access management, recognition of errors or abnormal software behaviour, susceptibility to social engineering, and commitment to practice policy and procedures. A form for recording all staff and their allocated computer and information security tasks can be found in the CISS Workbook, section 3.2.

Actions

- Computer security coordinator’s role description developed (refer to section 3.2.1).
- Staff member for computer security coordinator role selected.
- Computer and information security training for coordinator provided.
- Security coordinator’s role reviewed (eg. annually) and ongoing training provided.

Refer to CISS Workbook, section 3 for recording the roles and responsibilities of staff, the date for reviewing the coordinator’s role and the dates for training of the coordinator.
3.2.1 Practice computer security coordinator

The role of the practice computer security coordinator will vary depending on the IT skills of available staff, the availability of technical support and the interest of staff members. In some practices the principal general practitioner (GP) will take up this role, although it is better if it is delegated to one of the senior administrative staff, such as the practice manager. Most likely, the practice IT coordinator will also be responsible for computer and information security, and in many practices the roles will be shared by at least two people.

Role description

This position suits someone (or two or more people who share the position) who is enthusiastic about computers. They do not need to have advanced technical knowledge, although they should be reasonably comfortable with the operating system and relevant application software. They require management skills and the ability to develop computer security policies in consultation with others in the practice, with input from technical staff. Quite likely, they will also be the general IT coordinator for the practice. The tasks that are listed below should either be executed by the computer security coordinator, or this person should be aware which tasks the technical service provider is executing.

Responsibilities

The computer security coordinator role in a practice:

• oversees the development of documented computer security policies and procedures
• ensures the existence and testing of the computer business continuity and disaster recovery plans
• ensures that all policies and procedures are reviewed at least annually
• monitors and ensures that practice security policies are being followed. In particular that:
  – staff are following password security procedures
  – the routine backup procedure is in place and tested for data recovery
  – archived data remains capable of being restored
  – antimalware software is installed on all computers and virus definitions are automatically updated
  – the computers, especially the server, are adequately maintained and can deal with fluctuations in power
  – clear screen and clear desk policies are followed (ie. that screensavers are in place)
• maintains an up-to-date risk assessment including the IT asset register (hardware, software, licences, manuals and technical support)
• ensures technical advice is sought and acted upon for the installation of protection mechanisms such as intrusion detection and firewalls
• ensures secure messaging facilities are in place for the electronic transfer of information
• arranges ongoing security awareness training for members of the practice
• ensures the practice management is aware of any outstanding security issues and regularly report on security in practice management meetings.

3.2.2 Other staff roles and responsibilities
Other staff may also be assigned tasks related to computer and information security.
3.3 Practice security policies and procedures

Practices need to document their computer and information security policies and associated procedures. A policy is a reference document to the decisions that a practice has made about its security requirements and how these are managed. Policies should contain the overall objective of what is trying to be achieved, specific areas of responsibility, and the consequences of policy violations. The practice computer and information security policy can be in one or multiple policy documents. In addition to the policy, associated procedures giving specific details of how to implement the policy content should be developed.

A policy and procedures manual provides information and guidance to staff on the protocols in managing the computer and information systems. It is a source of information to clarify roles and responsibilities, and to facilitate the orientation of new staff. Confidentiality and privacy agreements for staff to sign; together with an appropriate computer use (of the internet, email and acceptable use) agreement should be included in this manual. All staff members and others, as identified in the risk assessment (refer to section 3.1), should sign these agreements. These act to protect the owners of the practice in the event of legal action against the practice arising out of a security breach that caused information to be released.

A policy and procedures manual also encourages practices to review and evaluate their computer systems and think through their requirements in both human and financial terms. The development of practice policies is informative and educative. Practices can engage in quality improvement and continuing professional development (QI&CPD) activities as they work through the issues. For instance, developing a ‘plan, do, study, act’ (PDSA) cycle will provide a framework for identifying and resolving issues.

Standard policy examples can be adapted for all areas of information security and it is unnecessary to create these from scratch. A description of the essential computer and information security policies are given in section 3.3.1. In addition, suggested staff confidentiality and computer use agreements can be found in section 3.3.2.

A computer and information security policy and procedures manual should include:

- the roles and responsibilities of the practice staff (clinical and nonclinical) in relation to protecting the practice’s information, and in particular the role of the practice computer security coordinator
- the risk assessment documentation including an IT asset register of hardware, software, and support services. This may include a record of digital certificates and their expiry dates
- the communication strategy to ensure that all staff are aware of any changes to policy and their responsibilities in managing computer and information security
• a complete set of policies and procedures for user activities which include
  – access for clinical and non-clinical staff
  – internet and email usage
  – acceptable use
• a complete set of policies and procedures for system activities which include
  – data storage including backup
  – malware (eg. virus) protection
  – wireless and mobile connections
  – perimeter controls and intrusion detection (eg. firewalls)
• a complete set of policies and procedures for general IT activities which include
  – business continuity plan including the disaster recovery plan. This is particularly important as it enables the practice to function when the computer systems are inoperable.
  – physical security (eg. restricted access to the practice server)
  – security management and reporting requirements.

Actions

✓ Computer and information security policies documented.
✓ Computer and information security policies reviewed annually.
✓ Associated computer and information procedures developed and updated as required.
✓ Staff trained in computer and information security policy and procedures.
✓ Individual staff agreement for confidentiality and computer use signed.

3.3.1 Practice security policies and procedures description

The practice manual should contain all the policies and procedures relating to the security aspects of the installation and use of computers, and electronic communication. Responsibilities for each component of computer and information security should be clearly defined, the policies should be clear, and the procedures should contain simple instructions that are easy to follow. It is of utmost importance to think through and discuss the contents of the manual within the practice, and ensure its implementation – it must not be left to just sit on a shelf.

All policies should have the following general structure:
• purpose and objectives of the policy
• scope of the policy (ie. to whom and what it applies, and under what circumstances)
• definition of computer and information security incidents and their consequences
• organisational structure and define roles, responsibilities and levels of authority
• reporting requirements and contact forms.
The necessary sections of the computer and information security policies manual will include:

**Risk assessment including security management and reporting (refer to section 3.1)**
This policy will detail the role of technical service providers. It also includes the monitoring processes that should be in place to ensure compliance with policies. Further, it will detail the vulnerability management, risk assessment and information security breach reporting procedures.

**Staff roles and responsibilities (refer to section 3.2)**
This policy contains information about the roles and responsibilities of practice staff. A practice computer security coordinator should be appointed and their role defined and acknowledged by the practice. The responsibilities of other staff with regard to computer security should also be defined. This will provide the basis for determining the level of access to each system. The practice computer security coordinator, who might be the general IT coordinator as well, should help ensure that staff are aware of the principles of computer security and are appropriately trained.

**Access control and management (refer to section 3.4)**
Access to systems should be consistent with the responsibilities outlined in the role description of each staff member. Each staff member should create his or her own password(s) for access. Passwords should not be written where they can be obtained by other staff or people who have access to the premises. The system administrator's password should never be divulged to anyone who is not authorised.

**Business continuity and disaster recovery plans (refer to section 3.5)**
A business continuity plan should first cover the critical functions of the practice so that in the event of a crisis the practice can continue without major disruption or risk to patients and staff. Second, the disaster recovery plan should contain the information necessary for returning the practice to its normal state. This will include using the backup as part of the recovery process.

The business continuity plan requires the creation and maintenance of an asset register that documents the hardware and software owned by the practice and details, where the computer media can be found, and who to phone for technical support. Maintaining a log of faults as they occur helps in dealing with computer problems, including ‘disasters’.

**Internet and email use (refer to section 3.6)**
Developing a practice policy that clearly states the management and use of internet and email by all staff within the practice will assist in mitigating security risks. This policy should also detail the practice policy on access to social networking websites such as Facebook and Twitter.
Backup (refer to section 3.7)
Details of backup and recovery procedures should be documented. The backup procedure is a key component of the business continuity and disaster recovery plans. Ensure that backup media are taken off site when the practice is closed. Record which members of staff perform the backups and automate as much of the procedure as possible. Data restoration should be tested periodically. If this is done by the technical services provider, then the computer security coordinator should ensure that it is being done on a regular basis.

Malware and virus protection (refer to section 3.8)
Malware and virus software installation and monitoring procedures should be documented. This should also include what to do if malware is detected.

Network perimeter controls (refer to section 3.9)
Network perimeter controls provide details of the systems (hardware and software) that protect the network. This may include firewall and intrusion detection hardware and software, content filtering and their related procedures.

Portable devices and wireless networks (refer to section 3.10)
This policy details the permitted use of portable devices within the practice. It also provides assistance on the factors that require consideration when installing and using wireless network access. Further, it should detail how and who can have remote access to practice systems (e.g., accessing practice information systems from home). This may include third party providers and access to practice systems via web-based portals.

Physical, system and software protection (refer to section 3.11)
Communicate to staff and record the practice policy on the use of screensavers and other precautions such as the positioning of monitors, to prevent unauthorised viewing of patient records and other confidential information. This policy also details restrictions of physical access for instance to the server, and how to secure equipment from theft and damage by power interruptions. In addition, it will detail the safe disposal of hardware and practice information. Document details of routine computer maintenance that is required. This includes hard disc ‘clean-ups’ (e.g., by a defragmentation utility program). It also addresses software maintenance procedures.

Secure electronic communication (refer to section 3.12)
Record the practice policy for electronic communication of patient records and other confidential information. This involves encryption and its associated procedures.

3.3.2 Sample confidentiality agreement
This sample may be used to ensure that practice staff and other people working in a practice, who may have access to confidential patient data or other business information, comply with privacy and security of information as required under legislation, including the Privacy Act 1988 (amended) and the National Privacy Principles. (This form can also be found in the CISS Workbook, section 3.3)
I (name) __________________________________ understand that as a condition of employment by (name and address of practice) _____________

I shall, neither during nor after the period of employment/engagement with the practice, except in the proper course of my duties or as permitted by the practice or as required by law, divulge to any person any confidential information concerning:

- patient personal, health and financial information
- the business or financial arrangements or position of this practice or any related company
- any of the dealings, transactions or affairs of the practice or any related company.

The contractual arrangement between this practice and its employees/contractors is founded on trust. I undertake not to knowingly access any confidential information about the business of the practice, patients or patient medical information, unless such information is essential for me to properly and efficiently perform my duties. I am aware that these conditions extend to unnecessary discussion of confidential information within the practice. I understand that any breach of this trust will render me liable to disciplinary action, termination and/or civil proceedings.

I further undertake to inform my supervisor immediately if I become aware of any breach of privacy or security relating to the information I access in the course of my duties.

This restriction ceases to apply to any information or knowledge, which subsequently comes into the public domain by way of authorised disclosure.

All confidential records, documents and other papers together with any copies or extracts thereof in my possession will be returned to the practice on the termination of my employment.

Signed: ________________________________

in the presence of

(Name) ________________________________

(Signature) ______________________________

(Position) ______________________________

Date: ________________________________
3.3.3 Contractual agreements

There is an onus on the practice to ensure that anyone who has legitimate access to the practice information is aware of their obligations to meet practice policies related to that information. Since technical service providers and those providing software and system support are usually granted unrestricted access to practice data, the following gives guidelines on what contractual agreements should contain.

Contractual agreements with technical service providers

Contractual arrangements with outsourced technical service providers should include:

- Data confidentiality – sensitive clinical and financial data must be kept private.
- Remote access – if the technical service provider accesses the network remotely, there has to be agreement on what they can or cannot view. If they can view ‘everything’, including files saved on workstations then all staff should be aware of this. Entities to whom information may be disclosed by a practice (or the types of entities to whom a practice would be likely to disclose information) must be stated in the practice’s published privacy policy. (Practices should obtain legal advice about this and other obligations under privacy laws)
- Backups and restoration procedures – what is the procedure? How often are the procedures tested? When is the ability to restore data tested?
- Response times – how long will it take the technical service provider to: Give phone advice? Provide assistance via remote access? Attend onsite? Provide after-hours assistance?
- Costs – what are the routine maintenance costs? What about additional work in case of a computer malfunction? What are the differences in costs in business hours and after hours?
- Regular maintenance – does the IT service provider undertake monthly server checks? Does the software provider perform software and drug updates and how often?
3.4 Access control and management

One of the key features of information security is information access by authorised personnel, appropriate to their role in the practice. Practices should develop a policy for who can have access to specific information and systems. This will be driven by the identification of potential system users in the risk assessment activity (refer to section 3.1).

It is essential to comply with governing privacy principles and all relevant state, territory and national privacy laws. Restricting access to those who are authorised will protect the practice against misuse of information.

Practices will need to develop their policy, after identifying and applying a risk analysis, to the needs of the practice. It is suggested that practices seek the support of suitably qualified technical service providers if needed.

Third party access for the provision of support and problem solving is an issue that requires careful consideration. This is often undertaken remotely and a great deal of trust is placed in software and support service staff. This should be underpinned by confidentiality agreements and the practice should ensure that the levels of confidentiality required are in alignment and enforced by the third party organisation.

Generally, there are five levels of role and responsibility-based access:

- Systems administrator: This level of access is usually the highest and often is only used by IT/security trained and external service providers for the server, operating system and network maintenance functions, and software support
- Practice manager: This access usually includes administrative functionality on the financial, clinical and network systems used in the practice
- Receptionist: This level of access is for patient administration such as appointments and billing.
- Clinical staff: This level of access is for use of the clinical programs. This access level may be further subdivided where delineation between the physician, nursing and allied healthcare staff access is required
- External or casual staff such as locums, researchers, students, software vendors and other healthcare provider organisations. This level of access will vary depending on the activities the person is undertaking.

A table for recording all staff, their access levels and permitted software access is provided in the CISS Workbook, section 4. Once a policy on access has been determined (ie. the rights, roles and permissions for staff), then practice staff can be given appropriate authentication methods. These can be divided into the following types:

- something you know (eg. a password, currently the most common means of authentication)
- something you have (eg. a token or smartcard)
- something you are (eg. a biometric profile – fingerprint).
Passwords are the most common form of access authentication. All staff must have their own passwords and not a shared common password. Best practice principles are that staff retain the responsibility for their own passwords and do not share them with other staff members; this includes not allowing staff to write down passwords and stick them on to monitors – which is unfortunately an all too common practice. Two-part authentication methods (a combination of two types of authentication) are significantly more secure.

A common problem in information security is the failure to remove the access rights of staff who leave the practice. It is important for the practice to consider the implications of staff who no longer work at the practice. The process for removal of access needs to be detailed in the access security policy and procedures manual. This will also form part of the policy relating to staff leaving the employment of the practice. A regular review of user access rights is important to also help detect where omissions have occurred or when staff have changed roles.

Other issues for consideration:

- Access to practice systems by external service providers. It is advisable to put in place a confidentiality agreement with anyone who works on or supports your computer system. This should include support for the practice computer system via modem or internet support. A suggested confidentiality agreement is given in section 3.3.2
- In addition to internal policies that are concerned with access rights and other data handling processes, privacy laws require organisations that deal with personal information to; make available to the public a policy about their data handling practices including collection use and disclosure. Practices should obtain advice about this and other obligations under state, territory and national privacy laws, and codes of conduct and indemnity or legal advisors.

Actions

- Staff policy developed on levels of access to electronic data and information systems.
- Individual staff are assigned an appropriate access level.
- Staff have individual passwords (not generic) which are kept secret and secure, and reset every 90 days or on a regular basis.
- Staff access removed when no longer working at the practice and passwords changed if required.
- Staff made aware of correct processes for handling and nondisclosure of passwords.
- Confidentiality agreements in place for third party and external access users.
- Demonstrable security and privacy policies of third parties to meet practice policies.
- Access monitoring and maintenance.

Refer to the CISS Workbook, section 4 to record access control and management information.
3.4.1 Setting access levels

Staff should only have access to the systems and information required to enable them to perform their role in the practice. All staff require a detailed position description that clearly outlines their roles and responsibilities and the required access to clinical and/or business information. Restricting access reduces the opportunity for accidents and errors. Staff will require appropriate training in the relevant computer software and the potential risks before access and passwords are provided. Additionally, healthcare identifiers (HI): healthcare provider identifier – individual (HPI-I) and healthcare provider identifier – organisation (HPI-O) should be recorded (for further explanation of these refer to section 3.12.1).

3.4.2 Access policy

The practice will need to establish an access and password policy that defines the user access level, password structure (number of characters) and the frequency with which passwords are required to be changed. All staff should create their own login passwords, and be responsible for keeping them secure.

It is also important for the practice to consider the implications of staff that terminate their employment, to ensure the decommissioning of passwords, remote access logins, and the return of computer equipment, backups and entry devices (keys) to the practice.

The access control policy should include guidance on:

- passwords
- management of guest account and remote access accounts
- termination of staff access

**Passwords**

The password policy should include the following aspects of password management:

- default passwords should be changed
- change passwords at regular intervals, eg. every 3 months
- minimum length (number of characters)
- use a mixture of alphabetic and numeric characters, and lower and upper case
- do not use familiar and family names or words that can be found in a dictionary
- do not use your date of birth
- do not reuse passwords
- do not disclose your password to anyone or allow others to use your login
- do not write passwords down and attach to screens.
Guest accounts and remote access accounts
Management of guest accounts and remote access accounts may include:
- the process to establish guest accounts
- the process to remove unused or unnecessary guest accounts.

Termination of staff access
A termination of staff access policy will detail the disabling or removal of access passwords and the return of entry devices (keys) to the practice management upon termination of the working relationship.
3.5 Business continuity and disaster recovery plans

Practical and implementable business continuity and disaster recovery plans are critical elements of computer and information security. With the increasing dependence on the information systems in general practice and access to information, these plans contribute to good governance processes within a practice. The management and recovery from a computer malfunction or security incident needs to be planned for. A business continuity plan will assist in minimising disruption, reduce risk to the business, and reduce the potential risk and inconvenience to your patients. This documented plan details what should be done when there are interruptions to the function of the computer system so that the practice can still function effectively, and focuses on prevention and recovery. The objective of clear and simple plans is that staff understand them and can follow them in disruptive events, a crisis or disaster situations. It is important that staff know their roles and responsibilities in such events.

Effective business continuity and disaster recovery plans are not about good documentation; they are about the processes the documentation describes. The benefits of good business continuity planning include reduced operational downtime, cost effective recovery, improved operational resilience, and effective and efficient processes.

As with the suggested risk assessment (section 3.1), the process for the development and implementation of business continuity and disaster recovery are based on current established standards and have been simplified to be implementable by the practice with minimal technical assistance. In larger organisations the process of development can take up to a year, whereas here the process has been shortened to avoid the lengthy consultations required for large organisations. These plans are distinct from the risk assessment process in that they focus on what happens after an incident has occurred. Risk assessment focuses on minimising potential damage and prevention of incidents.

**Business continuity**

A business continuity plan ensures continued practice operations when technical, environmental or intentional computer system failures occur. While the primary plan will concentrate on internal system malfunction or failure, the broader scenario should also be included, such as the functioning of the practice in the event of an environmental or natural disaster. This perspective is becoming increasingly important as e-health becomes a reality and medical practices become dependent on information transfer and the availability of crucial information. It must also be considered that a general practice exists beyond its own boundaries as it interacts with a wider healthcare community. In the electronic environment this specifically relates to the transfer of information to and from the practice to other healthcare providers (pathology laboratories, radiology providers, specialists and hospitals), new e-health services (electronic transfer of prescriptions) and government bodies (Medicare).
In the development of a business continuity plan, the first step is to identify the critical business functions and the resources required to operate the practice at a minimum acceptable level without functional computers. Therefore, the plan must include advice on how to revert to a paper based system until the computers are functional again, eg. a supply of prescription pads or paper.

A computer malfunction can be due to a number of factors including human error, hardware failure, software errors, and interruptions to power supply, malicious activity and environmental incidents. If a significant computer failure occurs, practices need to know how practice systems will be managed ‘manually’ and the information collected to be re-entered after recovery. These practice systems include:

- enabling clinical staff to provide adequate clinical care while not having access to electronic medical records
- appointment scheduling
- billing
- practice financial operations (payroll, Medicare claims).

The asset register is an integral part of the business continuity plan as it provides much of the essential information required to recover the practice computer systems quickly and efficiently. This will have been documented previously as part of the risk assessment process (section 3.1).

Lastly, training staff in business continuity procedures is vital, so that when a disaster occurs staff know what to do, what role and responsibility they have, and so that the practice can have confidence that it can safely handle adverse events. This training activity can be undertaken using practical exercises in the same way fire drills are practised, or using desktop walk through. Alternatively, such plans could be points of discussion at monthly staff meetings.

A business continuity plan development process can be found in following section 3.5.1, which leads you through the steps required and details the functions, resources, and procedures that are common to most general practices. The plan should be reviewed at specified time intervals, eg. annually or if something changes such as the backup medium or procedure. Forms for recording the relevant information in a plan, together with examples are provided in the CISS Workbook, section 5.

**Disaster recovery**

Data backup and restoration is one part of a business continuity plan and are referred to as disaster recovery. Backups are an integral part of the disaster recovery process. While disaster recovery is an integral part of business continuity planning there are specific actions that can be taken as precautionary measures such as, does the practice have a spare landline phone or mobile telephone for emergencies?; and where are the staff mobile numbers kept? Disaster recovery corrective procedure examples are provided in the CISS Workbook, section 5.
Actions

Business continuity and disaster recovery plans developed by:

- Identifying critical practice functions
- Identifying resources that will be required
- Documenting continuity and recovery processes including alternate work procedures for critical functions
- Assessing current preparedness and actions to be taken
- Educating staff about plans
- Business continuity and disaster recovery plans tested at specified intervals (eg. annually)
- Business continuity and disaster recovery plans updated at specified intervals and when technological or procedural changes occur
- Maintain fault log
- Print copies of completed plans and ensure staff know where to locate them in the event of an incident or disaster.

Refer to the CISS Workbook, section 5 for examples and forms.

3.5.1 Business continuity and disaster recovery

The business of general practice relies on a properly functioning computer system. A disaster recovery plan will detail the actions to be taken when the computer system, or any part of it, either stops functioning or is inefficient and impacts on the ongoing work of the practice. Business continuity refers to keeping the practice going, eg. making appointments and writing clinical notes. The development of a disaster recovery plan is usually in consultation with practice staff and the technical service provider. The computer security coordinator is responsible for managing this task.

An effective disaster recovery plan will bring the computer system back to working order, including the restoration of data. This is an increasingly technical and difficult area, and practices are well advised to consult a technical service provider.

Some failures in the computer system can be very simple. However, a disaster implies a major computer failure such as the server being inoperable. It is very important to know quickly when a computer problem can be fixed ‘in-house’ and when it requires assistance from a technical service provider.

A fundamental principle in developing plans is that they are simple to understand and follow. In general there are three levels of response: emergency, continuity and recovery.

- Emergency (first) response: This involves protection of people and property from immediate harm. These procedures will already be defined for the practice in the case of emergencies and natural disasters
• Continuity phase: The processes and procedures to ensure the practice continues to meet its critical functions at a minimum acceptable level
• Recovery phase: The processes and procedures to re-establish normal operation.

Note: The process described in this document has been condensed from prescribed business continuity theory and developed with reference to AS/NZS HB 292-2006 A practitioners guide to business continuity management. In order to make this exercise as practical as possible for the practice to undertake, the time consuming and generic steps in a formal business continuity plan formulation have been omitted or assumed. This includes the justification for having a plan; the critical success factors; a formal business impact analysis (the potential impact on the normal functioning of a practice has not been explicitly included as it is assumed that any nonfunctioning needs to be dealt with – regardless of the severity of the impact physically or financially); and resource interdependency mapping.

3.5.2 Development process and procedures
Business continuity and disaster recovery plans are formulated by performing the following steps.

3.5.2.1 Identify critical practice functions
These functions should include clinical and administrative functions. Identify the system/resources normally used to undertake this task and those resources that will be required in the event of the normal resources (the computer systems) being unavailable. A further consideration is noting any critical times of the month that activities usually have to take place. This may include payroll or end-of-month processes.

3.5.2.2 Identify additional resources that will be required for continuity and recovery
A practice needs to consider what organisational capacity and knowledge they already have in order to manage and implement the strategies detailed in the plans. What additional resources may be needed? To assist in identifying possible resource requirements, these have been categorised in the tables in the CISS Workbook, section 5.

3.5.2.3 Document continuity and recovery processes including alternate work procedures
This section has been structured to reflect the three phases of response: emergency, continuity and recovery.

Emergency response
The emergency and evacuation procedures will already be defined for the practice in the case of emergencies and natural disasters. First and foremost, these are in place to protect and preserve life.
Continuity phase
This phase concerns how to convert to manual procedures for critical practice functions. Each critical function in the practice requires a contingency plan so that when things go wrong the practice can continue to operate, and this includes the computer systems. Critical functions can be divided into either administrative or clinical. The practice needs to identify the major functions that are required to run the practice and how these will continue should the computer system be inoperable. The following are the elements that need addressing:
- laptop computer with copy of database on it – or copy of today’s appointments
- contact details and contact with patients
- work around processes (for all critical functions identified). Some procedures and examples are provided in the CISS Workbook, section 5.

Recovery phase
The recovery phase involves assessing the problem, corrective action, restoring the system, entering the backlog of information, communicating with those affected and a post-incident review. These tasks are discussed below.

Assess the computer problem
An assessment of the computer problem should be documented and include the following items:
- writing down or capturing (‘print screen’) any error messages
- note anything that has changed since the system last worked correctly
- check that all power and network connections and cables are plugged in and that the devices are turned on (check that lights are on).

Perform corrective action (with or without technical support)
These are some common computer ‘disaster’ scenarios in general practice. Complete the tables given in the CISS Workbook, section 5 and add any further items from your experience. Discuss them with your technical service provider. While these are listed as separate incidents it should be remembered that sometimes attacks have multiple components such as a Trojan (malware) installed which leads to unauthorised access.

It is important that the practice security coordinator knows the realistic capability of the practice to correct and recover from incidents to ensure that time is not wasted if technical assistance is required.

Restore system and reconfigure
The restore procedure is detailed in Section 3.7 (Backup). The information recorded in the risk assessment (eg. assets and their settings, users and their access levels) will be used for this. This task involves establishing procedures to test that the systems are functional. Systems checks will vary depending on the identified malfunction.
Enter backlog of information

This may need to be undertaken prior to resuming normal operations depending on the systems used in the practice and if information is required to be entered chronologically. Consultation with your software provider may be required to ascertain this.

A list of common tasks to assist you in planning what information will need to be entered or re-entered into the computer system, how this will be done and who will undertake this task, is given in the CISS Workbook, section 5. There should be plans for both entering data that was processed manually and includes re-entering data if the system had to be restored from a previous backup.

Note: In the event of short and medium term events, follow-up with external information transfer and exchange healthcare organisations may be necessary to ensure that any data that was transmitted during the time of nonoperation is transmitted again.

Communication strategy

Staff, patients, other healthcare providers, technical support providers and relevant authorities may need to be informed following an incident. Use the contact lists in Table 1 – User and technical contact details, in the CISS Workbook, section 2.3.

Review following recovery

Review the reason for the problem and ascertain how the recovery was executed, update the computer set up, document any important lessons, and update the policy and procedures manual. This step might involve modifying the software, backup process or acquiring new components. Further, consideration of insurance claims and policies may be necessary.

3.5.2.4 Assess current preparedness and actions to be taken

Assess and document (an action plan) what needs to be put in place to support the alternative procedures and access to additional resources. This will include the following:

• computer equipment redundancy
• people
• facilities
• communications
• data
• paper records
• technical assistance.
3.5.2.5 Educate staff about plans

Awareness and training is essential so that staff understand and are confident in what needs to happen should adverse events occur. The practice should decide how this will be undertaken.

Some suggestions:
• bi-yearly practical exercises (in the same way fire drills are practised or a desktop walk through)
• discussion at monthly staff meetings.

3.5.2.6 Business continuity and disaster recovery plans tested at specified intervals

Determine the interval or specific dates the plans are to be tested.

3.5.2.7 Business continuity and disaster recovery plans updated at specified intervals and when technological or procedural changes occur

It is important to keep the business continuity and disaster recovery plans current. This means updating them when new equipment is installed or when the practice procedures change.

3.5.2.8 Maintain fault log

Any fault or incident should be recorded. A form for this is provided in the CISS Workbook, section 5, Table 37.
3.6 Staff internet and email usage

There are many applications (programs) that can be installed that can be harmful to practice information and computer systems. While a significant amount of trust is put into all practice staff, it is remiss to disregard essential security measures that minimise potential risks in relation to staff usage of computer resources. Use of external applications, software and websites, and programs that can transmit information outside the practice pose a considerable security risk. This encompasses both the use of internet and email programs.

Communication of clinical information to and from healthcare providers should be done from within the practice’s clinical software using a secure clinical messaging system where possible. The use of a practice’s clinical software means that a record of communication is automatically retained in the patient’s record. In an exceptional circumstance where this mode of communication is not available and a message has to be sent via email, then the email message must be encrypted. Email normally transmits messages in readable, plain text formats, therefore it needs protection mechanisms such as encryption when used as a medium for transmission of data. Also, email is not a direct (point-to-point) transmission method as it passes through multiple servers to reach its destination. This results in the potential for interception and exposure of information if it is unprotected.

As social networking applications such as Facebook and Twitter have risen in popularity, the practice needs to be mindful of the desire of staff to be ‘constantly connected’. Therefore a reasonable use of internet and email policy should be provided. This will guide staff as to what is acceptable in the use of the practice internet and email. Limiting use of internet applications will also assist in defending against software attacks and subsequent necessity for support services to fix these. Methods for limiting internet use, to include or block specific sites and applications, can be setup by technical service providers. This is called white (permissible) and black (impermissible) website listing.

Suggested inclusion in an internet and email use policy can be found in the following section.

Actions
- Define acceptable use of internet and email.
- Periodic review of internet usage. This is to ensure that staff are not being hampered in their roles due to too stringent controls and policy.
- The use of email for transmission of health information is monitored and all messages encrypted.
3.6.1 Policies for the use of internet and email

The practice should develop a policy on what constitutes reasonable private use of internet and email by staff during office hours (i.e. use which does not interfere with work efficiency). Ensure that staff understands that using the internet at the practice should be for work related purposes only.

Make staff aware that emails sent from the practice to anyone at all, which might be construed as offensive or sexually harassing are not permitted.

If the practice is willing to communicate with patients via email or other electronic means, explain to patients and staff (eg. via the practice website if you have one or via the practice information brochure) any limitations to the timeliness and nature of the advice that can be provided. You should also explain if you charge any fees for electronic consultations. All such communication should be securely sent using encryption.

The practice needs to communicate to patients the way in which it will meet its privacy obligations. You should inform patients that no confidential information can be transmitted without encryption or other secure means. Similarly, you should explain that the practice requires their explicit request and permission to communicate in these ways. In addition to internal policies concerning access rights and other data handling processes, privacy law requires organisations that deal with personal information to make available to the public a policy about their data handling practices, including collection, use and disclosure. Practices should obtain legal advice about this and other obligations under privacy laws.

The practice policy will inform and guide staff on how to manage and use the internet and email. For example, is occasional personal use of the internet allowed? The policy must provide guidance to staff on the responsible use of these resources. The following may be included:

Internet use
- Internet use for business, clinical and research purposes only
- All downloads accessed from the internet must be scanned for viruses
- All sites accessed must comply with legal and ethical standards and practice policy
- Web browser security settings are not to be changed without authorisation
- Consequences of violations of the policy.

Email use
- Email use that breaches ethical behaviours and/or violates copyright is prohibited
- Do not send or forward unsolicited email messages, including the sending of ‘junk mail’ or other advertising material (email spam)
- All patient information sent via email must be encrypted
- All email communications should be treated as confidential
Do not use email for broadcast messages on personal, political or nonbusiness matters.

Be aware of phishing scams requesting logon or personal information (these may be via email or telephone).

### 3.6.2 Procedures for the safe use of internet and email

#### Protection against viruses
- Install and use antivirus and antimalware software, centrally installed where possible.
- Keep this software active at all times.
- Keep up-to-date by using automatic updates. Periodically, check manually that it is up-to-date.
- Apply patches to operating systems and application programs following technical advice.
- Do not download or open any email attachments where the sender is not personally known to you.
- Do not open unexpected email even from people known to you as this might have been spread by a virus.
- Use an antivirus mail filter to screen email before downloading.
- Do not use the ‘preview pane’ in your email program as this automatically opens your email when you click on the header.
- Save attachments and check for viruses before opening or executing them.
- Do not run programs directly from websites. Download files and check them for viruses first.
- Enable security settings in your internet browser to medium or high.
- Consider using internet browsers and email programs which are more secure.

#### Protection against the theft of information
- Do not provide confidential information by email – only do so via the internet when the site displays a security lock on the task bar and with an https in the web address.
- Use a second, non-critical email address when registering personal details where you are not completely sure of the site’s security.
- Do not inform people of your email password.
- Be aware of ‘phishing’ attacks. Phishing occurs when a website masquerades as a trustworthy entity, eg. a bank, in order to lure you into passing on sensitive information such as your username, password or credit card details.

#### Protection against hackers
- Install hardware and/or software network perimeter controls such as firewalls and intrusion detection systems between computers and the internet (following technical advice).
- If you install a software firewall, ensure that the practice knows how to use it.
- Ask the technical support person to test the firewall periodically and update it as required.
• If you are using a wireless network, seek technical advice on how to prevent others with similarly equipped computers hacking into the practice network.

Protection against spam
• Do not reply to spam mail
• Never try to unsubscribe from spam sites
• Remain vigilant: do not provide confidential information to an email (especially by return email) no matter how credible the sender’s email seems (eg. apparent emails from your bank)
• Use a spam filtering program.

Protection against spyware
• Learn how to recognise (and delete) spyware
• Do not accept certificates or downloads from suspect sites
• Install anti spyware software (from a reputable supplier).

Encryption of patient information
• Do not send patient information or other confidential data via email unless you are using encryption
• Be aware that encrypted files are not automatically checked for viruses. They have to be saved, decrypted and then scanned for viruses before being opened.

Backing up internet favourites or bookmarks and emails
• If you have a useful list of internet favourites or bookmarks make a backup of the list
• If you rely on information held in your emails make sure that it is backed up with the rest of your data.
3.7 Backup

Data can be lost through human error, software malfunction or failure, hardware problems and external causes such as theft. People can accidentally erase information, software can cause data loss through program flaws, and data storage devices can be lost or stolen. It is critical to make regular backups of all your information and software in case any of these occur. Also, the longer term preservation and access to health records needs to be maintained.

Storage and retrieval of information are a high priority in information security. A reliable and tested backup procedure is vital, as is the ability to restore all practice information after a computer incident. Knowing when to seek technical assistance is essential, and timely access to the latest backup (knowing where it can be located) is important.

The backup procedures are an integral part of the practice’s business continuity and disaster recovery plans (refer to section 3.5).

You need to know the answers to the questions below.

• What is your backup procedure?
• Which backup medium and software will you use?
• How can your backup data be restored?
• How can you check that the backup system works every time?

The installation of a backup system requires technical skills and is best provided by a technical service provider. There are several important points regarding backup and the backup procedures.

Choosing the appropriate backup software and hardware for individual practice circumstances is important. There are many types of backup media and programs to choose from and because of the rapid changing IT environment, practices should seek technical advice. Common backup media include read/writeable DVD/CD-ROM and portable hard drives. Also, in a networked environment the backup method can include transfer of data to another computer over the network or to an online backup service via the internet.

Backup media must be cycled so that at any point in time there are multiple backup copies of the practice data. If practicable, more than one backup method should be used. A suggested backup rotation strategy and recording sheet can be found in the CISS Workbook, section 6. A backup rotation is not applicable to networked or online backup.

The physical protection of backup media is important. It should be securely stored and access to it controlled. Leaving backups next to the computer or on desks is insecure. Make sure that backups are taken offsite and stored securely (eg. not left in cars or subject to heat). This includes knowing who has the most recent backup at any one time.
A distinction should be made between the daily backup (stored offsite and used to restore data when necessary) and weekly, monthly and yearly archives (used for long term data retention and legal purposes). All backups and archived data should be encrypted and password protected where possible and kept in secure locations. The distinction between system backups and business and clinical data backups are that business and clinical data backups need to be performed daily, while system backups are done less frequently as the operating system and software change less frequently.

Data restoration is the knowledge of how to ‘rebuild’ a system and server if it has become inoperable. It is not simply a matter of reloading the data; you also need documentation of which programs were on the computer and how they were configured. This needs to be done by or under the guidance of a technical service provider. The information contained in your risk assessment and asset register will be essential for this.

There are important issues to be considered regarding testing the backup and restoration procedures. A common problem is that the verification step of the backup process is overlooked or not checked that it has completed correctly. Unfortunately, this is usually only detected when it is necessary to use the backup for restoration purposes. It is vital that a staff member is responsible for checking that the backup has completed and verified correctly.

It is important that archive backups (weekly, monthly and yearly backups) can be read in the future. This becomes an issue when computer systems and backup methods are updated and replaced. A process for transferring archive backups to current backup media is required to ensure they can always be read by the currently available technology. The practice should be aware and meet the national and state records legislation in regards to the retention of patient information. The archive backups form part of this. The backup and long term record keeping policy for the practice should detail the local and national requirements. Further, these policies should ensure continuity of access to archived data and the processes for conversion of legacy system information to current readable formats.

**Actions**

- Backups of data performed daily, with weekly, monthly and yearly copies retained.
- Backups encrypted.
- Backups of data stored securely on and offsite.
- Backup procedure tested (by performing restoration of data) at specified intervals.
- Restoration procedure included in a documented business continuity and disaster recovery plan.

Refer to the CISS Workbook, section 6 for backup and restore procedure forms and examples.
3.7.1 Backup procedure

Backup and data restoration procedures are a vital component of the business continuity plan. However, as the optimal method of backup and restoration is quite technical, practices are advised to consult with an external technical expert on these matters. Document the backup process using the form provided in the CISS Workbook, section 6.

Any data and files that change should be backed up. This includes practice management and clinical systems data as well as documents, email files, internet favourites and bookmarks. You may require different backup and recovery procedures for each of these. While you do not need to back up your operating system or programs daily as these can be restored from the original media, it is a good idea to periodically backup the entire server. This can be done using disk imaging software as it takes an identical copy, or ‘image’ of your computer hard drive.

Note: It is important to keep a copy of the computer practice and policy procedure manual offsite so that if there is a systems failure, there is ready access to the restoration and business continuity procedures.

Further information on a step-by-step procedure for assessing and improving the procedures for backup can be found in articles such as Williams PAH. A practical application of CMM to medical security capability. Information Management and Computer Security 2008;16:58–73.

3.7.2 Backup media cycling

It is important to be observant for potential problems within the systems that manage data including backups. It is useful to have a series of backups so that you can restore a file from a point before the problem occurred. Having a system of daily, weekly, monthly and annual backups enables you to do this.

Daily backups – use a different tape, CD, DVD or hard drive. Label them by the day of the week, and use the appropriately named tape or hard drive, eg. Monday data is always backed up (overwritten) on the media marked Monday.

Weekly backups – have backup media labelled ‘Week #1’, ‘Week #2’. This should be used once every week of each month, eg. every Friday. Therefore ‘Week #1’ would be used on the first Friday of each month, ‘Week #2’ on the second Friday of each month and so on.

Monthly backups – have one backup media labelled ‘Monthly’. This should be used once every month, eg. on the first working day of each month.

Annual backup – this should be done at the end of the financial year.

Note: While this section gives details for physical media, network and online backup is also an option. This should not however be the only form of backup used. Consult your technical service provider for setup of network and online backup.
3.7.3 Documenting rotation of backup media
The backup rotation procedure will be dependent on the type of backup media and the process and software used. An example backup rotation schedule is provided in the CISS Workbook, section 6. This can be printed each month as a reminder of which media to use and record that the backup has been executed and checked.

3.7.4 Restoring data
In the event that the backup needs to be used to restore all or part of your practice data and programs, you need to document the process. In most instances this process will need to be actioned by your technical service provider or at least under his/her guidance. The practice policy on backup process should also include the procedures for keeping archived data (eg. yearly backups) to ensure that they are able to be read by current hardware.
3.8 Malware, viruses and email threats

Malicious code (malware) includes viruses, worms, and Trojans. Malware can have many purposes and intentionally seeks to corrupt, destroy or steal data, or to use your computer for unauthorised purposes. This may be to seek information about you and your practice, or to make use of your computer resources. Malware can interfere with computer functioning resulting in minor inconvenience or in extreme cases system inoperability. This can have a major impact on the practice through the loss or alteration of information. Certain types of malware can also capture your passwords (eg. key logging) and this is one reason why passwords should be changed regularly.

Malware is generally introduced into a system while communicating electronically with the outside world via email or the Internet. It can also be transmitted via CDs/DVDs, USB flash drives (memory sticks) and other portable devices and media.

There are various types of malware threats and these include:

• viruses and worms – malicious code that attaches itself to files and spreads from one computer to another
• Trojans – malware disguised as a real program.

In addition, there are also email threats that attempt to trick users into disclosing personal and login information. These include:

• phishing – fake emails and websites attempting to acquire usernames, passwords and credit card details
• spam – unsolicited or junk email. These are not a risk in themselves but they waste time to manage.

Another category of software programs includes tracking users and their internet habits. These include:

• spyware and adware – advertising supported and tracking software. It is used to collect information about a person or organisation without their knowledge, usually for advertising purposes
• cookies – small text files stored on your computer that keeps your login and other information, so that a web application or server can keep track of your activity. Cookies are not a security risk in that they are not malicious code or programs and cannot access the data on the computer. However, they can compromise the user’s privacy.

Certain types of software such as popular versions of internet ‘browsers’ or email programs allow easier downloading of viruses (and also expose computers to other security risks). Technical advice should be sought on whether changes to software settings would lower the risk of infection.
The risk of malware infection can be minimised by:

- having a process in place which minimises the risk of downloading malware, e.g. checking email attachments for viruses
- automatically updating antivirus and antimalware software
- monitoring staff activity and ensuring that policies on access and the use of the internet are followed. This will include staff trained not to respond or click on links in emails from unknown sources; to only open attachments where the source of the file is known; and to ensure all files downloaded from the internet are scanned for viruses.

Procedures for minimising the risks associated with internet use and email can be found in section 3.8.1 below, together with suggested procedures and policy inclusions. A form for recording your malware protection software and its renewal date is provided in CISS Workbook, section 7.

**Actions**

- Antivirus and antimalware software installed on all computers.
- Automatic updating of virus definitions enabled on all computers/servers.
- Automatic scans of computers are enabled.
- Staff trained in antimalware procedures as documented in the policies and procedures manual.
- Turn off the cookies feature in web browsers. Although some legitimate software may need this to function properly.

Refer to the CISS Workbook, section 7 for recording the details of the antivirus and antimalware software.

### 3.8.1 Malware and virus protection

The suggestions for this policy are to guide protection from malware. It should include:

- all computers attached to the practice network must have installed and enabled virus and malware checking software
- malware protection software that is not disabled or bypassed, nor the settings adjusted to reduce their effectiveness
- automatically updating malware protection software and its data files should be enabled for daily updating
- scanning all email attachments
- scanning all documents imported into the computer system
- weekly scanning of all computers
- training staff to deal with and report malware incidents.
3.9 Network perimeter controls

Network perimeter controls are the hardware and software tools used to protect the practice system by analysing data entering and leaving your network. It includes technical measures such as firewalls and intrusion detection systems. A balance between protections and allowing authorised remote access to practice systems needs to be in place. In network perimeter security, it is necessary to use multiple techniques and tools to protect the information systems and this is known as layering or defence-in-depth. This involves multiple protection mechanisms, such as firewalls, intrusion detection systems, VPNs, content filtering and antivirus protection.

Hackers can steal information and can cause mischief within your computer system and this can lead to the loss of data. You should consider the need for perimeter controls to be in the same category as the need for antivirus protection. They are essential for the long term protection of patient information; even an inadvertent breach may infringe privacy laws and doctor-patient confidentiality.

Firewalls

Firewalls check messages coming in and out of a network and block unauthorised access to a computer system. These can be in the form of software or hardware. A firewall is configured to a set of rules to allow and disallow messages to flow in and out of the practice network. It adds a layer of protection between the practice computers and the internet. A firewall can be software or hardware based. Unless you are using a standalone computer, it is advisable to install a hardware firewall for extra security rather than a software one. Firewalls need to be properly configured and periodically tested to ensure that they are still working. These are usually matters for a technical service provider.

Intrusion detection systems

Intrusion detection systems (IDS) monitor network and system activity to detect malicious and unauthorised actions and policy violations. They are usually software based and raise alerts if there has been unauthorised access to your systems. Intrusion detection systems do not prevent attacks on your system but they inform you that there is a potential problem so action can be taken. These systems are devices and programs that need technical knowledge to install and configure correctly.

Virtual private networks

Virtual private networks (VPN) provide a secure and reliable connection over the internet – sometimes referred to as a ‘VPN tunnel’. A VPN uses encryption to prevent unauthorised reading of messages (confidentiality), authentication to ensure only authorised users have access to the system being connected to (confidentiality) and that messages are not altered (integrity). It is most often used for remote access (access from outside the practice) to practice systems. Establishing this service requires technical assistance.
Content filtering
Content filtering is the use of software programs that can filter email and restrict access to the internet. Filtering for spam is the most common type of email filtering. Limiting access to known and trusted websites is commonly used.

Antivirus protection
An antivirus program also forms a component of network perimeter controls and is discussed in section 3.8.

Network perimeter controls are essential for anyone using the internet. Like viruses, unwanted intruders can invade your system. Your technical service provider can inform you about logs of unauthorised activity on your system. A form for recording the types and configuration of the network perimeter controls installed on your system can be found in the CISS Workbook, section 8.

Actions
- Hardware and/or software network perimeter controls installed and configured
- Hardware and/or software network perimeter controls tested periodically
- Intrusion activity logs monitored and breaches reported

Refer to the CISS Workbook, section 8 for the form to record the practice IDS and firewall configurations.

3.9.1 Network perimeter control policy
The network perimeter control policy and associated procedure will include access to network perimeter control hardware and software, its configuration and appropriate settings for the practice. This will need to be developed with assistance from your technical service provider or experts in this area.

All hardware and software perimeter controls used and their settings should be documented. Some of this information may already be recorded as part of the asset register in the risk assessment process.

3.9.2 Intrusion detection system
Record the hardware and software setup of IDS devices. These should be consistent with the network protection policies.

3.9.3 Firewall
Record the hardware and software setup of firewall devices. These should be consistent with the network protection policies.

3.9.4 Other controls
Other more sophisticated and complex controls may be required and these can be installed and configured by your technical service provider.

Other controls may include:
- use of hidden network addressing
- antimalware software installation on the firewall.
3.10 Portable devices and wireless networks

It is not enough to consider computer and information security only for the fixed hardware. Portable devices are increasingly being used inside and outside general practices. Remote access via wireless (Wi-Fi) connections and web-based access via internet connections make it easier to log on to the practice systems. In addition, the portability and small size of devices such as USBs mean that copying information is easier, whether for legitimate or unauthorised purposes. All portable devices should be password protected and encrypted where possible.

Portable devices include laptop computers, iPads, notebook PCs, USB flash drives, removable hard drives, mobile phones (particularly ‘smartphones’), personal digital assistants (PDA) and backup media such as tape. All of these are prone to being lost or stolen. These devices are a higher security risk as they are taken and used outside the more controlled practice location. This increases the risk of data inadvertently ending up with unauthorised people. Therefore, computer and information security measures need to be widened beyond the walls of the practice itself. Security for these devices can be increased using passwords and encryption. When not in use, these devices should be placed in secure locations.

Remote access to your practice computer system includes wireless networks and increases the convenience of access to practice information. However, it also requires additional security measures so that eavesdroppers cannot gain unauthorised entry to your computer system. There is increasing use of Wi-Fi (or Bluetooth) enabled laptops and other handheld devices, eg. for home and aged care visits, and you should obtain technical advice on how best to keep the equipment and information they hold secure. Wi-Fi devices must have encryption set up to ensure the confidentiality of information. Care should be taken when using devices in public places to avoid information being sighted, and connecting via open or unsecured public networks.

Remote access is also used by technical service providers to support your computer system. You should ensure that the methods used to access your system for IT support cannot also become security vulnerabilities. Procedures should be in place to minimise these risks such as the use of a VPN (section 3.9). In addition, since third parties may have access to your system legitimately, a list of suggested guidelines to include in a contractual agreement, as well as a sample confidentiality agreement for such providers is given in section 3.3.2 and 3.3.3.

Additionally, it is important to review the security for staff home computers where practice staff take electronic files home to work on them after hours and then return them to the clinic’s network. Data needs to be secured (encrypted) on portable devices as they can be easily misplaced or stolen. Care should also be taken for backup media which are taken offsite on a daily basis.

Forms for recording all portable devices that are used in the practice or to connect to practice systems, and your remote access setup can be found in the CISS Workbook, section 9.
Actions

❏ Portable computers and memory devices, including backup media need to be secured.

❏ Wireless networks (remote access systems) must be configured securely by an expert and should include:
  – encrypting the data transfer using WPA2 (Wi-Fi Protected Access 2) or stronger encryption standards to avoid information exposure
  – limiting the power of the router’s radio (Wi-Fi) signal so that it does not extend past the walls of the practice (known as the wireless footprint)
  – disable network broadcasting to reduce the risk of devices on the network announcing themselves to other devices on the network
  – enable media access control (MAC) address filtering to restrict unauthorised devices from connecting to the wireless network. A MAC address is unique to a specific computer or device
  – change the service set identifier (SSID) or the public name of the wireless network to something unique that does not identify the brand of device used or the business name.

❏ A policy on use of mobile devices in the practice should be developed. This would include the permitted devices and in what circumstances they can be used.

❏ Remote access should be set up using VPN connections.

Refer to the CISS Workbook, section 9 to list portable devices and their permitted use, and the setup of the practice’s remote access.

3.10.1 Portable devices

Portable devices may contain sensitive information or enable access to the practice server through remote means (wired or wireless internet connections). Ensure that the network cannot be hacked by unauthorised people. Seek external technical advice on how these can be secured.

Policy must include what devices are authorised to be used in the practice.

3.10.2 Remote access

The practice policy on remote access and use of wireless systems should be documented. Technical assistance may be required with this.

Aspects that should be considered include:

• allowable access channels (guest accounts, wireless, modem access)
• resources and system access allowed when using remote access
• disallow downloading or installing additional programs and utilities
• establish third party and vendor access rights and confidentiality agreements (see sections 3.3.2 and 3.3.3)
• use of a VPN for all remote access
• avoid public or open, unsecured networks.
3.11 Physical, system and software protection

Preventive strategies are required to keep the computer system running properly. It is best to have an arrangement with a technical service provider that includes routine network maintenance; do not treat their role as limited to providing emergency treatment when inevitable problems arise. There are certain maintenance procedures which, if performed regularly, will ensure that computers and other equipment run smoothly. The practice policy and procedures for these can be addressed as three separate areas.

- Physical protection and maintenance
- System maintenance (eg. the amount of free space on a hard disk)
- Software maintenance (eg. updates and patching).

Physical security

Location

Physical security is the first level of security defence. It provides protection from theft and unauthorised access. The physical location of the server is important, for instance locking it in a safe place or using antitheft steel cables. Desktop and laptop computers and other portable devices should always be kept physically secured. Locking away software, disks and backup media limits physical access. Do not position computer equipment beneath air conditioning units.

Heat and humidity

Environmental protection includes positioning computers, backup media and other components of the network where they are not subjected to excessive heat, eg. away from direct sunlight. All computers should be kept reasonably dust free, particularly over intakes for the cooling fans.

Uninterruptible power supply

Power outages and fluctuations can happen at any time. An uninterruptible power supply (UPS) is a device that contains commercial batteries that provide power to enable computers (especially servers) to shut down normally when the main electricity supply cuts out. This is important so that data that is being processed while the blackout occurs is not lost. A UPS also helps with power surges which can cause hardware damage. However, the batteries in most units only provide power for a short period of time, typically 10–30 minutes. In a prolonged blackout, the UPS should automatically shut the server down in an orderly manner to prevent data corruption or loss – it is not designed to continue running the practice systems. Prolonged blackouts require generators or other technical solutions which are likely to be beyond the resources of most practices. While a UPS should be installed on the main server, simple surge protectors are generally sufficient on other workstations in the practice. The network itself, including other devices attached to it such as modems, also need to be protected from power fluctuations that can cause data loss and hardware failure. The controlled shutdown procedure must be documented. Refer to the CISS Workbook, section 10.1 to record this procedure and details of the power protections installed the practice.
Secure disposal

Appropriate and secure disposal of old or decommissioned computer equipment, and importantly any data storage media especially hard disks, is vital. Password protection and/or encryption are not sufficient when disposing of old equipment. Disks and backup media should be securely erased (overwritten) or physically destroyed. There are many commercially available products capable of secure erasure. It is advised to seek advice from your technical service provider.

Recording removal of assets from practice

To reduce the potential loss or theft of equipment and assets, all removal from the practice premises should be formally recorded to minimise loss and theft. This will include recording the date out, date in and location when offsite. A predefined form for this is provided in the CISS Workbook, section 10.1.

Clear screen – computer screen confidentiality

This standard is not about privacy principles per se, although keeping information on the computer screen confidential is an instance in which a ‘privacy’ matter overlaps with information security. Information security in the consulting room is more about clinical staff behaviour than technical matters. For example, some doctors like their computer screens to be clearly visible to their patients during consultations. Nevertheless, doctors will have to decide if there might be sensitive information on the screen which should not be seen. For example, it might not be acceptable for a parent to see the past history of their adolescent child. More importantly patients should not be able to view the clinical record of another person, eg. the patient previously consulted. Similarly, receptionists need to be careful that patients do not have inappropriate visual access to any information on computer screens at the front desk. This includes ensuring that any medical and/or sensitive information read from the computer screen by receptionists is at an appropriate volume to maintain confidentiality.

There are various methods by which the information can be kept private. Common sense methods include remembering to exit the previous patient’s electronic file before the next patient enters the consulting room. Screen positioning can also help keep information private, including computers used by reception staff at the front desk. Other options worth considering are:

- the use of ‘clear screen’ function keys which instantly close down an open file. The following techniques are useful if you wish to suddenly leave the consulting room while the patient remains:
  - if using a Windows keyboard, pressing the Windows logo key and ‘D’ together will take you to the desktop. Rekeying these will take you back to your previous screen, or
  - pressing the Windows logo key and ‘L’ together will lock the screen forcing logging on again.
- the use of screensavers. These can be set so that you have to use your password to log back into your system
- logoff when leaving terminals or use automatic session time-outs.
Whichever method you consider most appropriate to your circumstances, the important thing is that staff are aware of how they can keep sensitive screen information from being inadvertently viewed.

**Clear desk policy**

To avoid accidental and unauthorised viewing of documents, it is effective to use a clear desk policy. At the least, this means at the end of each day staff clear their desks of all documents, notes and media. In addition, all documents should be removed from printers and fax machines immediately.

**System maintenance**

While some preventive system maintenance can be carried out by knowledgeable staff, most is usually undertaken by a technical service provider. The functions that this will include are checking disk capacity (hard disk space); defragmenting the hard disk when necessary; deleting and tidying up system and temporary files; checking error logs, checking that antivirus and other protective software is up to date; and documenting maintenance done on the system. An example of a system maintenance log can be found in the CISS *Workbook*, section 10.2. Simple system maintenance can be carried out by practice staff such as ensuring that areas near and around computer equipment is clean and dust free.

**Software maintenance**

This means performing ‘maintenance’ work on the computer system software on regular occasions. This can also include monitoring for signs of potential incidents using file integrity checking programs or using an external monitoring service.

- **Patching.** It is vitally important is keep the software up-to-date, especially your operating system software, eg. Windows. Patches and other program updates are essential to rectify security ‘holes’ in earlier versions. Many security experts agree that a large percentage of attacks on systems are through un-patched systems.
- **Restricting user access to avoid full administrative access will limit vulnerabilities to malware as this limits ability of users to install additional applications and programs, eg. from the internet. This also protects against unintentional modification of software configuration settings.**
- **Limiting access to system utilities to full administrative access only. Seek advice from a technical service provider for this.**
- **Software configuration.** Software also needs to be installed and maintained in accordance with the vendor’s guidelines to ensure security is maintained. This may also include ensuring that auditing is turned on, to log operating system and application activity as this information can be very useful when an incident occurs.
- **Run file integrity software periodically.** This software is sometimes provided by software vendor to check the integrity of the database and files.
- **Consider the use of an external network and system monitoring service.**
Unless you have sufficient technical knowledge amongst the practice staff, technical advice should be sought on how to keep your computer software functioning efficiently.

**Actions**

- Physical protection of the server and network is maintained.
- Uninterruptible power supply and surge protectors are installed.
- Practice staff are aware of how to maintain appropriate confidentiality of information on computer screens.
- System preventive maintenance should be undertaken regularly.
- Software updates and patches should be applied as soon as they become available.

Refer to the *CISS Workbook*, section 10 for relevant forms.

### 3.11.1 Physical

Clean around the back of computers and other equipment so that dust does not accumulate near the fans and power supplies.

In addition to protecting information you must also protect the computer systems physically. There are several components to this policy and associated procedures:

- restrictions of physical access to the server
- securing equipment from theft
- control the environmental conditions
- limiting damage by power interruptions
- secure disposal of hardware and practice information.

**Prevent unauthorised viewing of patient records and other confidential information**

There should be a policy on how to minimise and prevent unauthorised and accidental viewing of patient and practice information. This policy can include:

- the physical positioning of monitors in open access areas, consulting rooms and reception
- appropriate use of screensavers
- clear screen policy
- clear desk policy
- remove documents from printers and faxes immediately.

**Restrictions of physical access**

The practice computers and network are valuable and therefore limiting unauthorised personnel access to this equipment is recommended. The practice policy will document which personnel have authorisation to access such equipment.
Securing equipment from theft
All removable computer equipment should be secured from theft or damage. This is particularly important where equipment is in areas which are frequented by patients and visitors to the practice. This policy should include items such as:
- the use of cable device locks for notebook and laptop computers, and other mobile devices when in use in the practice
- lock laptops and similar equipment away at night if left on the premises
- do not leave USBs and software media in an insecure environment.

Uninterruptible power supply
The practice policy and procedures will document the use and maintenance of the UPS. The procedure for a controlled shutdown of the computer system should be clearly defined. Refer to the CISS Workbook, section 10.1.

Secure disposal of hardware and practice information
The practice policy and procedures should document the disposal of old, decommissioned and replaced hardware; particularly devices with any data on them. This could include:
- securely deleting all data on a device or media. Reformatting the media is not sufficient as forensic techniques can still access data on the device and media
- disposal of equipment through destruction.

Removal of assets from practice
Removal of all equipment and assets should be formally recorded to minimise loss and theft. This will include recording the date out, date in, and location when off site. A predefined template for this is provided in the CISS Workbook, section 10.1.

3.11.2 System maintenance
- Check hard drive capacity for the server
- Defragment hard disk at regular intervals
- Delete temporary files
- Check error logs
- Check that antivirus software is up-to-date and working effectively on all computers
- Keep a system maintenance log.

3.11.3 Software maintenance
- Add the latest patches to your operating system and application software
- Upgrade software as required
- Check for installation of unauthorised programs
- Create a procedure log
- Keep a software maintenance log.
3.12 Secure electronic communication

Securing electronic information is important to prevent it being read by an unintended recipient. While phone calls can be tapped, faxes can go to the wrong person and letters can be opened by a range of people at a practice or be delivered to the wrong address, electronic information transfer sets higher security standards. One reason is that electronic transmission makes it easier to inadvertently broadcast information to a wider audience. Another is that electronic transmission offers the opportunity to protect information more efficiently than previous methods of transmission.

Secure electronic communication is a broad term which includes secure messaging and the use of the internet. With the advent of e-health in Australia, and the potential for sharing information, secure messaging applies to all information transfer between healthcare providers, healthcare organisations, patients, and trusted third parties. There are broadly two types of information transfer and communication that are relevant to general practice:

- patient information transfer between healthcare providers, and between healthcare providers and trusted third parties using secure messaging
- communication via email – email is not a secure method of communication unless it is encrypted. Despite being a common communication method, its use needs to be carefully monitored. Mistakes such as incorrect addressing and the reliability of delivery need to be considered. Email is neither a direct nor an immediate communication method as email messages may be transmitted through multiple servers and networks en-route to the message destination, some of which will retain copies of the messages. Therefore, without strong identity and accountability using encryption such email can be intercepted, retrieved and read by without authorisation. To use secure email both the sending and receiving parties must use compatible encryption processes. Emails can legally be read by an internet service as messages pass through the provider system. This is in contrast to messages directly transmitted such as telephone calls and faxes, which are subject to interception legislation.

There are two aspects of encryption of messages sent via email or via a secure messaging system:

- encryption
- authentication.

Encryption means that data is electronically ‘scrambled’ so that it cannot be read unless the information is decrypted. Authentication means that one can verify whether the sender is who they say they are, and this is done by using electronic signatures. E-health information exchange in the Australian health system relies on, and incorporates encrypted, secure messaging techniques that are not necessary for practices to understand technically. The software programs used will handle this function are required to meet Australian standards.
What constitutes appropriate electronic messaging with patients is a question that every practice must address. Whether communicating via email, or via social networking sites (if the practice permits this) practices should ensure that data security remains paramount. Practices need to adopt a policy on the appropriate and safe use of email to ensure no privacy breaches – for both the practice and the patients. Given that most patients do not use encryption programs at present, emails between practices and patients need to be cautious and limited in scope, for both security and clinical safety reasons.

Encryption is technically easy for the end user once the system has been installed. However, until practices have access to encryption, it is advisable not to send confidential data via email or the internet. A suggested email and internet policy which includes security and safety considerations can be found in section 3.6. In addition, a template for recording the messaging keys in included in section 3.12.2.

**Practice website safety and security**

Practice website policies are a specific aspect of internet policies that are increasingly relevant in general practice. It is important that the information on practice websites is up-to-date and does not invite unsafe practices. For example, patients might wish to contact the practice via their website, but they need to be advised that sensitive clinical information should not be transferred in this way, and that there might be a delay in obtaining a response to their queries if they send a request in this way. The practice must abide by the Guidelines for Advertising of Regulated Health Services set by the Medical Board of Australia (http://www.medicalboard.gov.au/Codes-Guidelines-Policies.aspx).

There might be additional security risks if the practice website is hosted on the same computer that holds the practice data. If there is a security breach through the practice website there is a potential risk that the practice data would be vulnerable. Your technical service provider will be able to advise on the best methods to secure your website as this may require the use of a demilitarised zone (DMZ) which separates the website and services that patients may access, from the main practice systems.

The general practice website is a communication method that requires maintaining to ensure that the information held within the site is current and correct. The documentation includes identifying the timeframe for regular review of the website. The practice will need to identify which staff member is responsible for the practice website and document this in the staff member’s position description.

Email and internet policies, including that of practice websites help to ensure that confidential information is kept secure and private. Further, these policies will remind practices about the clinical safety concerns when providing advice to patients about serious health matters using electronic means.
4.1.2 Message system record

If more than one electronic communication method is used (for communication with different health organisations) each one should be documented separately. A form for recording the messaging systems used in the practice is provided in the CISS Workbook, section 11.
4 Conclusion

Computers are an integral part of general practice. Clinical and administrative information is now collected, stored and transmitted electronically, with an increasing number of practices no longer keeping paper files or records. As e-health initiatives become core to the provision of healthcare, the practice will need to review the processes that support patient privacy, and computer and information security. Increased connectivity provides increased opportunities for sharing information and improving patient care. Computer and information security is therefore not an option: it is an essential part of using a computer system in general practice.

Remember that there are three components to computer and information security:

• maintaining confidentiality
• ensuring the integrity of the information
• ensuring the availability of information when it is needed.

Computer and information security is a critical issue in the running of a practice and for protecting business and clinical information. The checklist and advice will assist the practice to maintain computer and information security standards, follow best practice and improve their information security processes.

The two most important elements of computer and information security for general practices are:

• appointing a computer security coordinator; and
• engaging a technical service provider who can assist in maintaining the system, and who is available at short notice to fix problems that cannot be fixed by the computer security coordinator or other staff in the practice.

Improving computer and information security in your practice requires adapting to an evolving technical environment, fostering staff awareness and gradually improving your protection processes. This standard is not intended to explain all the necessary technical aspects of security. You will need expert technical advice to assist you in some areas. The computer security coordinator should be aware of the role of technical service providers and the role they need to play in protecting your information systems. They need to know who and when to call for technical advice.

The computer security coordinator will also take on the responsibility for reviewing computer and information security on a regular basis (eg. annually) and for educating all practice staff in the practice’s policies and their responsibilities. All staff in the practice need to be aware of key issues in computer and information security; be able to recognise incidents when they occur; and adhere to the practice policy, follow security protocols and be appropriately trained.
Glossary of computer and information security terms

The following is a glossary of key technical terms relevant to computer and information security.

**Adware**: Free software that is supported by advertisements

**Availability**: Ensuring that authorised users have access to information when required

**Backup**: A copy of the files (system, software and data) in case the original is lost or corrupted

**Cache**: A cache stores recently used information for quicker access. The term is most commonly associated with the retrieval of web pages. A disk cache is an area of the computer’s memory that stores the most recently read information from the hard disk

**Client**: A client is a computer that requests services from a computer called a server, eg. in a network environment, a client would be your personal computer connected to the network. The client might request print services from a print server when you want to print a document or a file server when you want to access files

**Confidentiality**: Ensuring that information is only accessible to those who have authorised access

**Cookie**: A cookie is data sent to a computer by a web server that records browsing behaviour of the user

**Demilitarised zone (DMZ)**: A separation of an internal trusted network from the connection to untrusted external networks such as the internet. It provides an extra layer of security (using firewalls) where public or external access to services such as a website is required. It is also referred to as a perimeter network

**Denial of service (DoS)**: An attack that prevents or impairs the authorised use of networks, systems, or applications by exhausting resources

**Digital certificate**: A mechanism used to establish identity and authenticity of the message sender and/or receiver

**Encryption**: The process of converting plain text characters into cipher text (ie. meaningless data) as a means of protecting the contents of the data

**File integrity software**: Software that generates, stores and compares message digests for files to detect changes to the files

**Firewall**: A firewall is used to provide added security by acting as a gateway or barrier between a private network and an outside or unsecured network (ie. the internet). A firewall can be used to filter the flow of data through the gateway according to specific rules

**Hard drive (hard disk drive)**: A hardware device used for storing programs and data on a computer
Hardware: Physical components of a computer, such as a monitor, hard drive, or central processing unit (CPU)

Individual healthcare identifier (IHI): A unique identification number for individuals who seek healthcare

Healthcare provider identifier – individual (HPI-I): A unique identification number for healthcare professionals and other health personnel involved in providing patient care

Healthcare provider identifier – organisation (HPI-O): A unique identification number for organisations (e.g. a hospital or general practice) where healthcare is provided

Inappropriate usage: When a person violates acceptable use of any network or computer policies

Incident: A violation or imminent threat of violation of computer and information security policies, acceptable use policies or standard security practices

Information security: The protection of confidentiality, integrity and availability of information

Integrity: Safeguarding the accuracy and completeness of information

Internet service provider (ISP): A company that provides access to the internet

Local area network (LAN): A group of connected (networked) computers in the same location such as an office building or company

Log file: Contains records of events that have occurred automatically generated by the software or hardware

Malware: Malicious code is the term used to describe software programs that are designed to damage data or perform unwanted actions. It is used as the collective term for viruses, worms, Trojans and spyware

Mirrored hard disk: This is an additional hard disk that contains a mirror image of the original disk. If the original disk fails or becomes faulty, the mirrored disk can then be used

Modem: Acronym for modulator-demodulator: it is a device used to transmit computer information across the telephone network (by converting computer or digital signals into analogue signals and vice-versa). It can be used to allow users to connect to the office network while they are away from the office (e.g. at home or travelling), or to connect computers to the internet via a dial-up or broadband connection to an ISP

Network: A collection of connected computers and peripheral devices used for information sharing and electronic communication

Network drive: In the simplest case, a network drive is a complete hard disk/drive on a network server that is made available to users on the network
Network interface card (NIC): Also called a network adapter, an NIC is a hardware device (located inside the computer) that allows the computer to connect to a network and communicates with other computers on the network.

Nonrepudiation: This term means that you cannot deny having performed a transaction, eg. if you send an email to your bank asking them to transfer money out of your account, nonrepudiation means you cannot later deny having sent the email. Use of encryption and digital certificates provides nonrepudiation capabilities.

Operating system: Software that communicates with the computer hardware at a basic level, allowing application software to function. For example, Macintosh™, Windows™ and Linux are types of operating systems.

Peripheral device: A device attached to a network or a computer that provides input and output such as a keyboard or a printer.

Proxy/proxy server: A server that all requests from computers on a local network have to pass through to access the internet. It can improve internet access speeds as it uses caching to save recently viewed web pages, images and files. It also acts as filter for what is allowed into the local network.

Redundant array of independent disks (RAID): A method for storing data on multiple hard disks in a computer. This can improve performance and fault tolerance.

Reboot: When you restart your computer. You might be required to reboot your computer in some instances, eg. after installing new software to enable the changes to take effect.

Registry: A database used by Microsoft Windows to store system configuration information about the software installed on a computer. It should never be tampered with unnecessarily as this can lead to your computer not functioning properly.

Remote access: The ability to gain access to a network or system that is not in the same physical location.

Rootkit: A group of programs and files designed to gain unauthorised access to a computer using full administrative privileges.

Router: A device that provides connectivity between networks, eg. between your internal network and the internet. A router forwards data from one network to the other and vice-versa. Many routers also have built-in firewall capabilities.

Server: Typically a computer in a network environment that provides services to users connected to a network (or ‘clients’), such as printing, accessing files and running software applications. A server can be used as a central data repository for the users of the network.

Social engineering: An attempt to trick someone into revealing information (eg. a password) that can be used to attack systems or networks.
Software: A program or (group of programs) which performs specific functions, such as word processor or spreadsheet programs

Spam: Unsolicited or junk email. Often it is simply nuisance email, but it can entice you to provide confidential personal information, eg. banking passwords

Spyware: Programs that are downloaded from the internet onto your computer (sometimes without your knowledge) to covertly send back information eg. your personal details, to the source

Standalone computer: A computer that is not connected to a network or to other computers

Threat: A potential event that could cause harm to the information or the information system

Trojans: Unauthorised programs hidden within authorised ones

Unauthorised access: Attempting to gain access without permission to a network, system, application or data

Uninterruptible power supply (UPS): Battery backup to maintain power for specified time period during power outages

Uniform resource locator (URL): The address for an internet website, page or file, such as http://www.racgp.org.au

USB flash drive: A memory data storage device integrated with a USB (Universal Serial Bus) interface

Virus: A malicious software program that can create copies of itself on the same computer and on others

Virtual private network (VPN): Creates a secure connection (using encryption) between specific locations or networks across the internet or a wide area network

Vulnerability: Weakness in an information system that could be exploited by a threat

Wide area network (WAN): A network that is not restricted to a local area. Using telephone lines, fibre-optic cable and satellite links, it can span long distances

Wi-Fi: Wireless networking standard that enables transmission of data over wireless networks

Wi-Fi protected access (WPA): A method using encryption to create secure wireless (Wi-Fi) networks

Wi-Fi protected access 2 (WPA2): A more advanced and secure method using encryption to create secure wireless (Wi-Fi) networks than WPA

Worm: A self-replicating computer program worm (similar to a computer virus) that uses the network to send copies to other computers

Zero day exploits: A malicious computer attack that takes advantage of security vulnerability before it is known or patched