

2005-2006 Security Awareness and Conformance Report – Action Guide

Action Guide

The following table provides basic information and guidance for implementation of the Security Awareness and Conformance Report. Documents such as those developed by the GPCG on security and firewalls will provide additional information.

Tasks	Action Guide
Practice IT security coordinator's role description written (for GP, existing staff member or practice manager)	<input type="checkbox"/> Security management and operational responsibilities are to be documented such that they are understood by all staff and can be allocated to individuals with the appropriate skills.
Practice IT security coordinator appointed	<input type="checkbox"/> Security management and operational responsibilities are to be allocated to individuals with the appropriate skills. It is critical that an individual(s) are appointed the responsibility of oversight of Practice security.
IT security training for coordinator provided	<input type="checkbox"/> Individuals with IT Security responsibilities should possess the appropriate skills to fulfil the responsibility. This may include hands-on knowledge of IT security policies, risks and mitigators and formal IT security training courses. <input type="checkbox"/> The responsibility of IT Security for Practice's may include the procurement of specialist skills for either selected or all IT security functions.
Security Coordinator's role last reviewed	<input type="checkbox"/> The role is to be reviewed at least annually or in the cases of significant technology change or in response to new IT security threats.
Person(s) (e.g. IT security coordinator) appointed to document (and revise) security policies and procedures (can be part of practice manual)	<input type="checkbox"/> The role description of the IT Security coordinator includes the function of documenting Practice IT security policy and procedures. This is to be reviewed at least annually or in the cases of significant technology change or in response to new IT security threats.
IT security policies and procedures documented	<input type="checkbox"/> The Practice shall have IT security policies and procedures documented in either standalone manual or as part of its Practice manual. The GPCG security guidelines provide a first step for Security policy. Specific practice standards and procedures will need to be developed to implement.
IT security policies and procedures documentation last reviewed	<input type="checkbox"/> The documentation is to be reviewed at least annually or in the cases of significant technology change or in response to new IT security threats to ensure efficacy and adequacy.
Staff trained in IT security policies and procedures	<input type="checkbox"/> All staff shall receive security awareness training and specifically the Practice IT security policy and procedures. This should occur as an induction function for new staff and an annual refresher course for all staff. This should include a process of staff signoff on an understanding of Practice policy and procedures and of their individual responsibilities.
Staff policy developed on levels of electronic access to data and systems	<input type="checkbox"/> An access control policy should be documented that details the access rules applicable to various staff functions and various information types (classifications). This should implement the responsibilities under information privacy laws. In summary this will be to restrict access to information on a business needs to know basis. Access to Personal health records shall be limited to staff that need to access the material as a function of their role in the flow of patient care. <input type="checkbox"/> Access control functions shall be implemented in computer systems consistent with the defined policy. This may include creation of server directories with differing accesses, logon restrictions to clinical applications or the implementation of application security to control accesses within the application. Most, but not all systems will have some security functionality to control access.
Staff have created personal passwords to access appropriate level	<input type="checkbox"/> Access to information systems such as LAN servers, laptops and application systems shall be via unique Userid/password pairs (as a minimum) with each user's password being known only to the staff member to which it is allocated. <input type="checkbox"/> User passwords shall be changed immediately upon allocation by the User to a password determined by the User that can be memorized.
Passwords are kept secure	<input type="checkbox"/> Passwords should ideally be memorized and not stored in ways that could be easily obtained by other persons or programs, i.e. do not write on Post-it Notes left on computer screens, desks or secreted in areas where they could be uncovered. <input type="checkbox"/> Passwords should not be shared between Users where accountability for system access or action is required.
Consideration given to changing passwords periodically	<input type="checkbox"/> Passwords should ideally be changed based on the frequency of use, sensitivity of information that may be compromised and the risk of compromise over time. This is a defense against a number of technical and non technical attacks on passwords, such as multiple attempts of access over time (known as brute force password attacks), keystroke logging etc. <input type="checkbox"/> Passwords frequency change options should be enabled on computer systems. The frequency of change of 120 days may be a reasonable period for General Practice that creates a culture that does not resist password change enforcement. More frequent change may be appropriate for sensitive information.
Disaster recovery plan developed	<input type="checkbox"/> A strategy shall be developed and procedural details documented for the recovery of IT computer systems in the event of a disaster. This may be as simple as ensuring routine system backups are taken and kept offsite such that computer information is retrievable in the event of a disaster such as fire. The plan should include details of how computer systems will be restored, e.g. new servers procured and restored to a new or replacement practice environment. <input type="checkbox"/> A strategy may involve the contracting of disaster recovery services or specialist skills if desirable.
Disaster recovery plan tested	<input type="checkbox"/> The plan should be tested at least annually that may involve the testing of server recovery procedures and the restoration of data and application systems. <input type="checkbox"/> Testing may involve the contracting of disaster recovery services or specialist skills if desirable
Disaster recovery plan last updated	<input type="checkbox"/> The disaster recovery plan shall be reviewed and updated annually and in response to changes to computer systems impacting plan execution, i.e. server or other computer infrastructure changes.
Practice aware of need to maintain appropriate confidentiality of information on computer screens	<input type="checkbox"/> Computer screens should be positioned so that contents are not easily viewable by the public

2005-2006 Security Awareness and Conformance Report – Action Guide

Screensavers or other automated privacy protection device enabled	<input type="checkbox"/> Secure screensaver options should be enabled for desktop/laptop systems (windows or other operating system functions) such that they blank any sensitive data and lock unattended systems after a period of activity. Ideally this may be after 15 minutes of inactivity for screens that may be more accessible to unauthorised people or longer periods if this period impacts productivity or performance of practice staff. <input type="checkbox"/> Session locking option at either LAN/server operating system or within application security should be enabled similar to the periods for screensaver. Additional third party security products for desktop and laptop security can be purchased that may apply greater protection in <i>locking down</i> these devices.
Back-ups of data done daily	<input type="checkbox"/> Implement a backup procedure that backs-up data that has changed since the last backup. It is likely that a backup each night of server data or changes (incremental backup) is desirable for Practices. The period between backups may be longer if the Practice considers the risk of failure and its ability to recover or recreate data between backups is achievable (e.g. once a week backup). <input type="checkbox"/> A procedure may implement a scripted backup to a tape unit whereby a manual procedure to eject the backup tape occurs. Backups may be done over a communications link to an alternate location or may be undertaken as a procured service offering via an ISP (Internet Service Provider) or ASP (Application Service Provider).
Back-ups of data stored offsite	<input type="checkbox"/> A tape/disc backup or a tape/disc backup replica is to be securely stored offsite to be used for disaster recovery in the event of destruction of computer systems and local backup media.
Back-up procedure last tested (by performing a restoration of data)...	<input type="checkbox"/> Back-up restoration procedure is to be routinely tested to ensure the currency of the restore procedure and the efficacy of the backups. This may be accommodated within the testing process of the disaster recovery plan. Backup tape efficacy may also be proven on a more regular basis or on an adhoc basis through restoration of corrupt or deleted data. Obviously any failure in the backup process in this context will result in an in-ability to recover to the last good backup.
Back-up procedure has been included in a documented disaster recovery plan	<input type="checkbox"/> Back-up restoration procedure is to be included in DRP.
Anti-viral software installed on all computers	<input type="checkbox"/> Anti virus product is installed on all personal computers, laptops and servers. <input type="checkbox"/> Full system scans are conducted weekly on all devices.
Automatic updating of viral definitions enabled (daily if possible)	<input type="checkbox"/> Licenses are current and virus signatures are downloaded as soon as there are available from software vendors. Ideally a <i>live</i> update facility should be employed and configured such that the updates are automatically downloaded when available
Staff trained in anti-viral measures as documented in policies and procedures manual	<input type="checkbox"/> Staff awareness and procedures and in place for response to virus infections such that staff limit the likelihood of spreading a virus
Hardware and/or software firewalls installed	<input type="checkbox"/> Ensure firewall is installed between internal network and insecure public network such as the Internet. <input type="checkbox"/> Ensure no other un-firewalled connections to insecure networks exist, i.e. creating an unprotected backdoor into your LAN. All communications traffic to and from the internal network must be routed through the firewall as the only route. <input type="checkbox"/> All ports not required are turned off. Only required ports to be activated in rules. The default rule is to deny all connections to and from the internal network and authorise specific connection via firewall rules. Refine rules as desired to restrict inbound and outbound ports and restrict services to identified network addresses for services. Refer configuration guidance on the site and vendor configuration guides.
Hardware and/or software firewalls tested	<input type="checkbox"/> Check firewall rulebase each month to ensure it is current and applicable. Audit or engage an IT security specialist to confirm firewall is protecting against known computer hacking scenarios.
Computer hardware and software maintained in optimal condition (includes physical security, efficient performance of computer programs, and program upgrades and patches)	<input type="checkbox"/> Ensure hardware and software is kept up to date with patches as soon as possible after release. Processes will need to be put into place to monitor update releases. In some cases vendors may provide a notification or online update service. Focus on server and PC operating system security patches, and security products including anti-virus, network security and firewalls. <input type="checkbox"/> Where possible ensure network equipment and in particular the firewall, is physically secured from unauthorised access. This may be in a lockable room.
Uninterruptible Power Supply (UPS) installed (to at least the server)	<input type="checkbox"/> Implementation of standalone UPS device on critical server(s) for graceful shutdown period is advantageous in the event of a power outage. Assess Practice requirement if this is cost/benefit-risk justifiable. If the impact on computer systems or practice function of power loss is not significant it may be justifiable to accept the risk of an outage. In same cases the building power supply may be UPS protected providing battery/generator power for a defined period.
Encryption systems considered - Encryption used for the electronic transfer of confidential information	<input type="checkbox"/> Transmission of sensitive health information over the Internet (a public network) potentially exposes the information to unauthorised access. Encryption when emailing of health records over public networks should be implemented. This may require the exchange or cryptographic keys or certificates. <input type="checkbox"/> Encryption of file transfer or other application level data exchanges of Health records over public networks should be implemented. This may require applications to implement security protocols such as SSL (Secure Sockets layer) or IPSec (Internet Security Protocol) and may require the exchange or cryptographic keys or certificates.