

## Online System Security Policy

*Current as at 21 December 2001*

### General

1. Responsibility for online security and site compliance with Commonwealth security guidelines must be part of the duty statement of an officer in AFTRS responsible for information technology management.
2. AFTRS Security Plan must be drafted, where appropriate, in accordance with the PSM and ACSI 33 guidelines and describe the necessary security mechanisms and procedures that should apply to any AFTRS website or online system, including all of the key services that are involved in delivery of a website or online system (eg DNS, firewall, databases, Internet link).
3. The relevant AFTRS managers must be aware of the appropriate DSD security contacts and established incident reporting systems, so that when an incident does occur the correct reporting procedure is followed.

### Security Audit or Review

1. A formal Threat and Risk Assessment must be performed against any AFTRS website or online system every 12 months by an appropriately qualified body or AFTRS.

### Privacy

1. Any AFTRS website or online system must have a prominent privacy statement making clear what information is collected and how it will be used, and warranting that any information collected will be securely protected from unauthorised disclosure.
2. Any AFTRS website or online system must contain a privacy statement that complies with all the online Privacy Principles developed by the Privacy Commissioner.

### Government Classified Information

1. If or where Government Non-National Security Classified information (eg In-Confidence, Protected) is made available on any AFTRS website or online system, then only DSD approved security products that have been evaluated under the Australasian Information Security Evaluation Program (AISEP) must be used; and/or the aggregated security mechanisms and procedures must provide adequate protection of the data (refer to the PSM, ACSI-33, and DSD guidelines).
2. No National Security Classified information must be available on any AFTRS website or online system.

### Encryption and authentication

1. If or where any AFTRS website or online system makes use of a Public Key based encryption or authentication technology, that technology must meet the mandated Commonwealth Gatekeeper standards and must be sourced from Gatekeeper accredited suppliers.
2. If or where any AFTRS website or online system uses strong, digital signature based authentication to identify or authenticate business customers online, the websites or online



3. systems must use the Australian Business Number (ABN) as the identifier and the Gatekeeper compliant ABN-Digital Signature Certificate as the authentication tool, as is mandated for Commonwealth agencies.

## External Hosting / Service Providers

1. All non-AFTRS external third parties (eg web hosts, outsourcers, web developers, telecommunications providers, payment gateway providers) with a substantial role in the delivery of any AFTRS website or online system, or the handling of sensitive site information, must be accredited according to AS 4444, or demonstrate compliance with Commonwealth security guidelines such as ACSI 33 or the PSM.
2. Where non-AFTRS external third-parties play a role in directly managing or updating any AFTRS website or online system, procedures must be in place within AFTRS (eg Service Level Agreements with suppliers, contract conditions) to ensure effective protection of the confidentiality of site data, preservation of site security, and best practice site management.

## System Auditing

1. A detailed audit and activity log collection and review system must be in place on any AFTRS website or online system, including associated Internet systems.
2. Online system audit or activity logs must be scanned, analysed and archived regularly.
3. Incident analysis must be performed and recorded where suspicious activity is evident.
4. AFTRS must be a participant in an established incident reporting system.
5. Systems and procedures must be in place to report suspicious or damaging activity to DSD or appropriate authorities under the incident reporting framework.

## Intrusion Detection

1. Intrusion detection and/or network monitoring systems must be in active operation on any AFTRS website or online system.

## Information Protection

1. Where information about individuals or businesses (including e-mail addresses) is collected by, or available from any AFTRS website or online system, appropriate measures must be in place to securely store and protect this information.
2. Access control, authentication and protection mechanisms must be in place on sensitive elements of any AFTRS website or online systems. Mechanisms may include:
  - IP address or Domain Name access restrictions;
  - proxy server access controls;
  - restrictive file/directory permissions;
  - security measures on data bases behind firewalls;
  - user authentication of web site visitors and users;
  - encryption used for authentication, confidentiality or integrity.
3. Systems must be in place to detect unauthorised changes to any AFTRS website data and key system configuration files.
4. Systems must be in place to capture and report illegal, unusual and unexpected input to any AFTRS web server or other online system elements.



5. Regular backups of site content and key system data must be performed, and stored securely.
6. A disaster recovery plan for AFTRS websites or online systems must be prepared and tested, which should include planning for recovery from a serious website security breach or system failure.

## Change Control

1. Relevant system changes must be reviewed and tested from a security perspective before implementation.

## Firewalls/Sanitisation

1. A formal sanitisation and checking process must be employed when information is transferred from the internal network to any website in order to guard against leakage of sensitive information.
2. Firewall(s) must be in use to control access to any AFTRS website or online system, from external and sensitive internal systems, and to also block unauthorised transmissions from the site.
3. Any firewall(s) in use on sensitive system elements must be certified by DSD or an appropriately qualified organisation.
4. Firewalls in use must be actively maintained and monitored, and the latest updates, patches etc must be applied.

## Additional Web Server Functionality

1. If or where any AFTRS website or online system uses active server content or technologies (such as CGI scripts, ASP, PHP, Java servlets, Cold Fusion, or Server Side Includes) appropriate measures must be in place to identify, and then remove or control any vulnerability these technologies may introduce.
2. If or where any AFTRS website or online system provides an ability to query or display information from a database product (such as SQL Server, Oracle, DB2, Access), appropriate measures must be in place to identify, and then remove or control any vulnerability this functionality may introduce.
3. Any additional online functionality or Internet services (such as telnet, email, FTP, chat, NNTP, LDAP directory services) offered by any AFTRS website or online system must be identified, appropriately authorised, protected and managed, under the same security arrangements that apply to the core services of any AFTRS website.
4. The relevant AFTRS manager must audit or scan all AFTRS websites or online systems for any common vulnerability that may be introduced into an online system, where technologies such as active server content, databases or other Internet services may be made available. AFTRS information technology manager must take remedial action to address any vulnerability that is identified.

## Site 'Hardening'

1. On any AFTRS website or online system, no software or services other than those required to deliver the core functionality of the site should be installed.
2. On any AFTRS website or online system, sample code normally installed as part of the default set-up of any web server and/or operating system must be removed.

3. On any AFTRS website or online system, development tools must not be installed, or if installed, must be appropriately secured.
4. On any AFTRS website or online system, remote administration tools or web pages must not be installed or active. If installed or active, they must be appropriately protected with, for example, IP address or domain name restrictions on their use, or access must only be made available via an authenticated encrypted session.
5. On any AFTRS website or online system, there must be a procedure in place to ensure that vendor security patches/updates for key system software components (the web server, operating system, database, middleware etc) are regularly applied.
6. On any AFTRS website or online system, passwords must be changed regularly, and there must be clear guidelines in place for password selection and usage for all systems involved in delivering the service, including advice to staff not to disclose passwords to unknown third parties.
7. Administrative access (physically and electronically) to the externally visible or key elements of any AFTRS website or online system (eg the 'live' web server or the firewall) must be tightly restricted.