



Australian Government

Department of Finance and Deregulation

Australian Government Information
Management Office

FedLink GATEWAY

SELF REVIEW GUIDE

VERSION 3.0

AGIMO ICT Security Team

Phone: (02) 6215 1585

Email: fedlinkenquiries@finance.gov.au

AGIMO ICT Security Team
John Gorton Building, King Edward Terrace,
Parkes ACT 2600

November 2007

Table of Contents

TABLE OF CONTENTS	2
INTRODUCTION	3
PURPOSE AND SCOPE	3
INSTRUCTION ON THE USE OF THE GUIDE.....	3
SELF REVIEW ACKNOWLEDGMENT	4
ANNUAL SELF REVIEW	4
SELF REVIEW PROCESS	4
RISK ASSESSMENT	5
RISK ASSESSMENT PROCESS	5
IT SECURITY POLICY.....	5
IT SECURITY POLICY DOCUMENT	5
DEVELOPMENT OF THE DOCUMENT	5
GATEWAY MANAGEMENT	6
MINIMUM ADMINISTRATION PROCEDURES.....	6
ACCOUNT ADMINISTRATION.....	6
BACKUP, MAINTENANCE AND MEDIA CONTROL	6
CHANGE CONTROL	7
INCIDENT REPORTING	7
PHYSICAL SECURITY	7
ARCHIVE REQUIREMENTS	8
RECOVERY OF GATEWAY SERVICES	8
GATEWAY DESIGN.....	8
FURTHER READING.....	9
GATEWAY SELF REVIEW STATEMENT OF COMPLIANCE	10
AFTER HOURS CONTACT:	10
RISK ASSESSMENT	11
SECURITY POLICY DOCUMENT	11
GATEWAY ADMINISTRATION PROCEDURES	12
CHANGE CONTROL	13
INCIDENT REPORTING	13
PHYSICAL SECURITY	14
ARCHIVES REQUIREMENTS	14
RECOVERY OF GATEWAY SERVICES	15
GATEWAY DESIGN.....	15
ACCEPTANCE OF SELF REVIEW BY AGENCY.....	16

Introduction

1. The Information Security Group (ISG) of the Defence Signals Directorate (DSD) has developed this guidance document on behalf of the Australian Government Information Management Office (AGIMO). AGIMO is the Australian Government manager of FedLink. The requirements outlined in this guide are consistent with the minimum information security requirements for X-IN-CONFIDENCE detailed in the Commonwealth Protective Security Manual (PSM) 2005 and the Australian Government Information Technology Security Manual otherwise known as ACSI 33 (Sept 2007)

Purpose and Scope

2. The Gateway Self Review Guide is intended for use by Australian Government Agencies and others (herein referred to as agencies) authorised to apply to connect to the FedLink network at all X-IN-CONFIDENCE levels **except CABINET-IN-CONFIDENCE**. Agencies planning to connect to FedLink at PROTECTED level cannot conduct a Self Review. These agencies should see the I-RAP Gateway Certification and PROTECTED Level FedLink Connection Guidelines & Checklist at URL: www.dsd.gov.au/library/, or seek a Commercial Gateway Service Provider that has current DSD Gateway Certification to PROTECTED level and approval to connect to FedLink.

3. Agencies connecting at the X-IN-CONFIDENCE level only do not require DSD or I-RAP Gateway Certification; instead agencies can choose to conduct a FedLink Gateway Self Review.

4. Agencies with a current formal DSD or I-RAP Gateway Certification or that are hosted by a Commercial Gateway Service Provider with DSD Gateway Certification and approval to connect to FedLink do not require any further certification for connection to the FedLink network and are exempt from completing a self-review until the period of their existing certification expires.

5. This guide identifies those aspects of FedLink Gateway implementation and management that as a minimum must be considered by agencies. The guide also provides a Self Review Statement of Compliance that agencies are required to complete before connecting to the FedLink network and return to DSD.

Instruction on the use of the Guide

6. In using this guide agencies must:
- a. Follow the guidance provided in paragraphs 12 to 30;
 - b. Develop and implement the appropriate policies, plans and procedures;
 - c. Have the Statement of Compliance signed by both the agency Information Technology Security Manager (ITSM) or Information Technology Security Adviser (ITSA) and the appropriate business manager; and

- d. Forward a copy of the completed Statement of Compliance together with an electronic copy of completed documentation to DSD
7. Agencies may choose to use a commercial service provider to assist in the self-review process. AGIMO recommends the use of an endorsed I-RAP assessor.

Self Review Acknowledgment

8. DSD will acknowledge receipt of the Statement of Compliance and documentation and forward a copy of the acknowledgement to AGIMO. At this point the self-review process is complete and, pending AGIMO connection prerequisites have been met, connection to the FedLink network can occur.

9. After the self-review has been completed, claims made by an agency against the requirements of the FedLink Gateway Self Review Guide may be audited. AGIMO may choose to conduct the audit, or advise the agency to seek the services of an I-RAP assessor. The audit will be performed in consultation with the agency.

Annual Self Review

10. Once a self-review is completed and connection to the FedLink network has occurred, agencies are required to either complete an annual self-review or obtain DSD or I-RAP Gateway Certification or have their gateway services hosted by a Commercial Gateway Service Provider with DSD Gateway Certification and approval to connect to FedLink. If the agency decides to conduct self-review again it is required to complete the Statement of Compliance once again and forward it to the ISG together with an electronic copy of the agency's gateway documentation.

Self Review Process

11. The self review process comprises 4 stages:
 - a. Undertaking of a risk assessment,
 - b. Development of IT security policy documentation,
 - c. Determination of how the gateway will be managed, and
 - d. Completing the Statement of Compliance.

Security Risk Management Plan

12. Risk management is a process for comprehensively and systematically managing risk in an organisation. Gateway security risk management follows the same principles and processes as risk management, but the risks are specific to gateway security.

13. The Risk Assessment is an important component of an organisations risk management.

14. The organisation MUST conduct a risk assessment on the gateway environment.
15. The risk assessment MUST contain:
 - analysis of the risks;
 - categorisation of the risks including target risk levels/predetermined standards; and
 - risk treatments.
16. The risk assessment MUST have been signed by the CEO or delegate of the organisation confirming they have read and accepted the risk assessment, including the identified residual level of risk.
17. ACSI 33 March 2007 (Part 2 - Chapter 2) describes the steps in a risk management process.

System Security Plan

18. The System Security Policy (SSP) is a document that details how all relevant security policy will be implemented for a given ICT system. As part of the gateway self certification process, the SSP will contain the high level security architecture of the gateway and the policies that need to be enforced within the system in order to mitigate the risks identified in the Security Risk Management Plan.
19. The System Security Plan should be developed with reference to ACSI 33 and NIST 800-18 *Guide for Developing Security Plans for Federal Information Systems*, and as a minimum, should contain the following subsections:
 - 1) Management Controls – Risk Assessment Methodology, any previous Security Reviews of the Gateway.
 - 2) Operational Controls – including personnel security, physical and environmental security, Contingency planning, Application Software controls, Data Integrity and Validation Controls.
 - 3) Technical Controls – Identification and Authentication, Logical Access Controls, Public Access Controls and Audit Trails.
20. A template is included in Appendix A to assist with the development of the System Security Plan.

Gateway Management

Minimum Administration Procedures

21. Agency management is responsible for ensuring that all gateway administration staff understand and implement the administrative procedures. These procedures must be consistent with the policy from which they are derived.
22. As a minimum the following procedures must be developed and implemented:
- a. Account Administration,
 - b. Access Control,
 - c. Backup, Maintenance and Media Control,
 - d. User Awareness,
 - e. Change Management,
 - f. Physical Security,
 - g. Incident Response,
 - h. Archive Requirements, and
 - i. Recovery of Gateway Services.

Account Administration

23. User and administration accounts should be created using strict procedures. Such procedures will include:
- a. Password lengths,
 - b. Permission to grant accounts,
 - c. Password lifecycle,
 - d. Password storage, and
 - e. Details of privileged accounts that are required, and who is allowed to hold these privileged profiles.

Access Control

24. Access Control should be managed using strict procedures. Such procedures will include:
- a. Access control requirements for a system, and
 - b. How to perform access control changes.

Backup, Maintenance and Media Control

25. The backup procedures should:
- c. Detail those systems that require backup (a system could be a server, host or application);

- d. Include the frequency of backup, storage of tapes/disks and period of storage, media reuse/disposal;
- e. Involve developing a backup plan to include backup or archiving of logs or audit trails.

26. Media Control addresses the procedures for recording, storing, sanitising, declassifying and disposal of media.

User Awareness

27. The user awareness procedures should detail the mechanisms for initiating and maintaining a program so that users are aware of their responsibilities.

Change Management

28. A formal change control process must be developed and implemented. The change control process must have formal procedures for testing changes and a formal process for review and approval of changes.

Physical Security

29. Agencies connecting to FedLink must have as a minimum an ASIO Security Construction and Equipment Committee (SCEC) approved intruder alarm in place within the physical environment of the gateway. Agencies should also develop procedures for access control to the gateway computer systems. Where possible the FedLink encrypting router should be collocated with other critical gateway devices. ACSI 33 March 2004 (Part 3 – Chapter 1) contains further information on physical security requirements.

Incident Response

30. The incident response plan must detail:
- a. broad guidelines on what constitutes an incident,
 - b. the minimum level of training for users and system administrators,
 - c. the authority who is responsible for initiating investigations of an incident,
 - d. the steps necessary to ensure the integrity of information supporting a compromise,
 - e. the steps necessary to ensure that critical systems remain operational, and
 - f. how to formally report incidents.

31. All Category 3 or higher incidents must be reported to ISG as soon as practicable through DSD's Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS). Definitions of incident categories can be found at the OnSecure web site: www.onsecure.gov.au/.

Archive Requirements

32. All security related logs must be retained for the length of time specified in the National Archives Act of Australia 1983, Administrative Functions Disposal Function, Sub Section Technology and Communications, Reference 2099¹.

Recovery of Gateway Services

33. Agencies must develop a plan that outlines the procedures involved in recovering gateway services in the event of a failure occurring in the operation of the gateway. Potential failures should have been identified as part of the risk assessment.

Gateway Design

34. All services passing through the gateway must be denied by default unless expressly permitted. The decision to allow a service through the gateway must take into consideration the risk assessment and the gateway policies.

35. All traffic between the internal FedLink servers and the Internet must be routed through a firewall that is listed on the DSD Evaluated Products List (EPL)² as evaluated to EAL2. The configuration of the firewall must be in accordance with the products Security Target (ST) and Certification Report (CR). Management of that firewall must be via a secure, authenticated link.

36. Agencies connected to FedLink are required to:
- a. Develop system(s), and/or
 - b. End user education policy, plans and procedures

to mitigate the high risk of end-users sending classified information over the Internet in error wrongly assuming that the source and destination are in FedLink and are cleared to the security level required.

¹ At the time of this guide being written, the Act specified that the logs be kept for a minimum of 7 years.

² EPL http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html

Further Reading

Australian Government Information Technology Security Manual (also known as ACSI33), March 2004.

<http://www.dsd.gov.au/library/infosec/acsi33.html>

Gateway Certification Guide Version 3.0, 2004

<http://www.dsd.gov.au/library/infosec/gateway.html>

National Archives Act of Australia 1983

Commonwealth Protective Security Manual, 2000

Gateway Self Review Statement of Compliance

Agency Name: _____

Address of Gateway
Location: _____

Postal Address: _____

IT Security Manager: _____

Phone Number: _____

Fax Number: _____

E-mail Address: _____

After Hours Contact: _____

Risk Assessment

	Yes	No
A risk assessment has been undertaken for the agency gateway	<input type="checkbox"/>	<input type="checkbox"/>
The risk assessment identifies:		
a. key system assets	<input type="checkbox"/>	<input type="checkbox"/>
b. all threats that may reasonably occur	<input type="checkbox"/>	<input type="checkbox"/>
c. consequence/harm profile against each threat	<input type="checkbox"/>	<input type="checkbox"/>
d. the current risk for each asset/threat pair	<input type="checkbox"/>	<input type="checkbox"/>
e. an acceptable risk level for each asset/threat pair	<input type="checkbox"/>	<input type="checkbox"/>

Comments: _____

Security Policy Document

	Yes	No
A security policy document has been developed for the agency gateway	<input type="checkbox"/>	<input type="checkbox"/>
The security policy document contains the following sections as a minimum:		
a. Access Policy	<input type="checkbox"/>	<input type="checkbox"/>
b. Administrative Security	<input type="checkbox"/>	<input type="checkbox"/>
c. Personnel security	<input type="checkbox"/>	<input type="checkbox"/>
d. Physical security	<input type="checkbox"/>	<input type="checkbox"/>
e. Communications and Key Management security	<input type="checkbox"/>	<input type="checkbox"/>
f. Equipment maintenance and disposal	<input type="checkbox"/>	<input type="checkbox"/>
g. Normal and Privileged Access to Systems	<input type="checkbox"/>	<input type="checkbox"/>
h. Media Security	<input type="checkbox"/>	<input type="checkbox"/>
i. Configuration and change control	<input type="checkbox"/>	<input type="checkbox"/>
j. User Responsibilities and Awareness	<input type="checkbox"/>	<input type="checkbox"/>
k. Contingency planning	<input type="checkbox"/>	<input type="checkbox"/>

I. Incident Response

The security policy document contains clear links to the risk assessment

Comments: _____

Gateway Administration Procedures

The following gateway administration procedures have been developed as a minimum:

- | | Yes | No |
|--|--------------------------|--------------------------|
| a. Account administration | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Access Control | <input type="checkbox"/> | <input type="checkbox"/> |
| c. Backup, maintenance and media control | <input type="checkbox"/> | <input type="checkbox"/> |
| d. User Awareness | <input type="checkbox"/> | <input type="checkbox"/> |
| e. Change Management | <input type="checkbox"/> | <input type="checkbox"/> |
| f. Physical Security | <input type="checkbox"/> | <input type="checkbox"/> |
| g. Incident response | <input type="checkbox"/> | <input type="checkbox"/> |
| h. Archive requirements | <input type="checkbox"/> | <input type="checkbox"/> |
| i. Recovery of Gateway Services | <input type="checkbox"/> | <input type="checkbox"/> |

Other developed gateway administration procedures:

- | | Yes | No |
|---|--------------------------|--------------------------|
| All gateway administration staff are aware of all developed gateway administration procedures | <input type="checkbox"/> | <input type="checkbox"/> |
| All developed procedures have been implemented in practice | <input type="checkbox"/> | <input type="checkbox"/> |
| All procedures are consistent with the agency security policy document | <input type="checkbox"/> | <input type="checkbox"/> |

Comments: _____

Backup, Maintenance and Media Control

	Yes	No
A backup plan has been developed	<input type="checkbox"/>	<input type="checkbox"/>
The backup plan details systems which require backup	<input type="checkbox"/>	<input type="checkbox"/>
The frequency of backups and period of storage are detailed	<input type="checkbox"/>	<input type="checkbox"/>
Backup plan includes backup or archiving of logs or audit trails	<input type="checkbox"/>	<input type="checkbox"/>
Media control procedures include recording, storing, sanitising, declassifying and disposing of media	<input type="checkbox"/>	<input type="checkbox"/>

Change Management

	Yes	No
A formal change management process has been developed	<input type="checkbox"/>	<input type="checkbox"/>
The change management process includes formal testing procedures	<input type="checkbox"/>	<input type="checkbox"/>
The change management process includes a formal process for review and approval of changes	<input type="checkbox"/>	<input type="checkbox"/>
All gateway administration staff are aware of change management procedures and implement them within their positions	<input type="checkbox"/>	<input type="checkbox"/>

Comments: _____

Incident Response

	Yes	No
An incident response plan has been developed	<input type="checkbox"/>	<input type="checkbox"/>
The incident response plan details:		

- broad guidelines on what constitutes an incident,
- the minimum level of training for users and system administrators,
- the authority who is responsible for initiating investigations of an incident,
- the steps necessary to ensure the integrity of information supporting a compromise,
- the steps necessary to ensure that critical systems remain operational, and
- how to formally report incidents.

All gateway administration staff are aware of the correct procedures to follow when an incident occurs

All gateway administration staff understand the requirement to report all Category 3 or higher incidents will be reported to ISG as soon as practicable

Comments: _____

Physical Security

A minimum of an ASIO SCEC approved intruder alarm has been put in place Yes No

Other physical security measures in place:

Comments: _____

Archives Requirements

Understand the requirement to retain logs in accordance with the Yes No

National Archives Act of Australia, 1983

Procedures in place to retain and appropriately store logs for the required period of time

Comments: _____

Recovery of Gateway Services

	Yes	No
Policies, processes and procedures are developed and implemented to ensure recovery of gateway services	<input type="checkbox"/>	<input type="checkbox"/>

Comments: _____

Gateway Design

	Yes	No
All services passing through the gateway are denied by default unless expressly permitted	<input type="checkbox"/>	<input type="checkbox"/>

All traffic between the internal FedLink servers and the Internet is routed through a firewall that is listed on the DSD Evaluated Products

List (EPL) as evaluated to EAL2	<input type="checkbox"/>	<input type="checkbox"/>
The configuration of the firewall is in accordance with the products Security Target (ST) and Certification Report (CR)	<input type="checkbox"/>	<input type="checkbox"/>

Management of the firewall is via a secure, authenticated link

Systems have been developed, tested and implemented to mitigate the high risk of end-users sending classified information over the Internet

AND/OR

End-user education policy, plans and procedures are in place to mitigate the risk of end-users sending classified information over the Internet

Comments: _____

Acceptance of Self Review by Agency

By completing this form the agency states the following:

- a. The gateway complies with all the requirements of this document,
- b. The agency agrees to manage the gateway in a secure manner,
- c. The agency accepts any responsibility should the gateway be compromised,
- d. The agency understands that FedMAC may choose to have the FedLink connection audited within the period of this connection, at which time the agency will be required to contact ISG, which may choose to conduct the audit or advise the agency to seek the services of an I-RAP assessor to conduct the audit.

Signed by the Agency ITSM _____

Printed Name _____

Date Signed _____

Signed by the Agency CEO or delegate _____

Printed Name _____

Date Signed _____