Annex B: Defence Gateway Security Operating Procedures

Introduction

1. This document constitutes the Security Operating Procedures (SyOPs) for the Defence Gateway, a component of the JSF facility. They are issued by the System Security Officer (SSO) in accordance with MOD Departmental Security Regulations, and have been approved by the DAIS Accreditor. All personnel using Defence Gateway are to read, understand and comply with these SyOPs and no departure from or amendment to them is permitted unless the SSO gains prior authorisation from the Accreditor.

2. Disciplinary action will be taken against those personnel who breach or ignore these orders. Any incident that has, or is likely, to compromise the security of Defence Gateway is to be reported immediately to the JSF SSO, DGW helpdesk or the JSF SAC.

Scope

3. Defence Gateway is designed to provide an OFFICIAL single sign on solution to Defence personnel. It is hosted on the Joint Server Farm which is accessible via the Internet, but can also be accessed by means of RLI connected machines through the MOD Enterprise Gateway Service (EGS).

Acceptable Use

4. All DGW Users are to comply with the MOD's Acceptable Use Policy[1]. In summary Users are not to:

a. Attempt to access areas where they are not authorised to access;

b. Attempt to damage the system to prevent its use;

c. Attempt to introduce software or hardware of any type without consent from the JSF SAC and accreditor;

d. Make unauthorised modifications to the system or the information hosted on it.

Classification

5. Defence Gateway is a controlled area accessible only to authorised users and may be used to share OFFICIAL information. Specific areas such as MODBOX are also able to support the handling instruction of SENSITIVE. Information of a higher classification must not be placed on Defence Gateway in any form. If such information is identified, users should notify Defence Gateway (admin@armymail.mod.uk) and their unit security officers immediately. For details of the Classification Marking Scheme[2].

Email & Attachments

6. Users are responsible for ensuring that all emails they send comply with the following rules:

---

[1] JSP 740 Acceptable Use Policy

[2] JSP 440 Part 4 Section 1

a. Users may send emails (and attachments) that are OFFICIAL to recipients located on MoD systems, the Public Switched Network (PSN) and the Internet. They should note that unmarked information may still be sensitive and must be given the protection they think it merits, respecting any handling instructions which have been added.

b. If there is a need to send emails over the internet at OFFICIAL-SENSITIVE it must be in accordance with MOD Policy/Guidance.

c. Document files may contain previously deleted, Protectively Marked classified information hidden within the file. All documents to be attached to email should first be cut and pasted from the original document into a new file and the new file attached to the email.

d. The email capability should only be used for business requirements accept for where there is a need to use it for welfare purposes.

Roles and Responsibilities

7. The roles and responsibilities of the Defence Gateway are detailed below:

a. **Defence Gateway Domain Administrators.**

(1) Maintain patch levels of supporting software.

(2) Act as Senior User Manager.

(3) Act as 2nd and 3rd line Support.

(4) Report any suspect activity to the DGW Helpdesk (admin@armymail.mod.uk) , JSF SSO/SAC (Army Info-IS-IAS-Gov-ComplSO3).

b. **Defence Gateway Application Administrators.**

(1) Act as 1st Line Support.

(2) Act as User Manager for DGW Users in their group.

(3) Report any suspect activity to the DGW Helpdesk (admin@armymail.mod.uk), JSF SSO/SAC (Army Info-IS-IAS-Gov-ComplSO3).

c. **Defence Gateway Users.**

(1) Maintain own details.

(2) Report any suspect activity to the DGW Helpdesk (admin@armymail.mod.uk), JSF SSO/SAC (Army Info-IS-IAS-Gov-ComplSO3).

d. **Application Managers.**

(1) Maintain own details.

(2) Create user accounts.

(3) Maintain applications.

Passwords

8. Passwords are controlled by Defence Gateway. Passwords must be a minimum of 8 characters and must be alpha numeric with upper and lower case. Passwords are reset every 6 months and have a history recognition of 3.

9. Password resets are initiated by the user and use a challenge response setup during registration.

10. Users are also required to maintain and update their Security Question and Answers.

11. Passwords are not to be shared with anyone or written down anywhere under any circumstances.

Monitoring/Auditing

12. Use of the DGW is, and will continue to be, subject to monitoring. Users are advised that system logs are checked on a regular basis in order to detect unauthorised or suspicious system and security events.

13. DGW administrators have the right to gain access to user accounts in case of an emergency or a legitimate legal/business requirement. A detailed request is to be provided by the requestor of exactly what they are requesting access to and for what purpose. This must be agreed with the user's line manager and recorded for audit purposes. Once the access is granted the extraction of information must be carried out within legal guidelines and a 2 man rule must be followed[3][4]. Dependant on the circumstances, all reasonable attempts will be made to inform the DGW user of the request to access their account. Access to their account is to be conducted by the users Line Manager or the delegated authority given by the system owner.

14. Anyone suspected of breaching the Acceptable Use Policy or detected misusing their privileges through monitoring may be subject to disciplinary or even legal action[5].

Cookie Policy for Defence Gateway

What Are Cookies?

15. As is common practice with almost all professional websites, the Defence gateway and sites within uses cookies. Cookies are tiny files that are downloaded to your computer, to improve your experience. This information describes what information they gather, how we use them and why we sometimes need to store these cookies. We will also share how you can prevent these cookies from being stored, however this may downgrade or 'break' certain elements of the sites functionality.

For more general information on cookies see the Wikipedia article on HTTP Cookies.

How We Use Cookies

16. We use cookies for a variety of reasons detailed below. Unfortunately in most cases there are no industry standard options for disabling cookies without completely disabling the

[3] Telecommunications (Lawful Business Practice Regulations) (Interception of Communications) Regulations 2000

[4] Data Protection Act 1998

[5] JSP 740 Acceptable Use Policy.

functionality and features they add to the Defence Gateway. It is recommended that you leave on all cookies if you are not sure whether you need them or not in case they are used to provide a service that you use.

Disabling Cookies

17. You can prevent the setting of cookies by adjusting the settings on your browser (see your browser Help for how to do this). Be aware that disabling cookies will affect the functionality of this and many other websites that you visit. Therefore it is recommended that you do not disable cookies.

The Cookies We Set

18. If you create an account with the Defence Gateway then we will use cookies for the management of the sign up process and general administration.

19. We use cookies when you are logged in so that we can remember this fact. This prevents you from having to log in every single time you visit a new page. Cookies also support the Single Sign on functionality.

20. From time to time we offer user surveys and questionnaires to provide you with interesting insights, helpful tools, or to understand our user base more accurately. These surveys may use cookies to remember who has already taken part in a survey or to provide you with accurate results after you change pages.

21. When you submit data to through a form such as those found on contact pages or comment forms cookies may be set to remember your user details for future correspondence.

Third Party Cookies

22. In some special cases we also use cookies provided by trusted third parties. The following section details which third party cookies you might encounter through this site.

23. We may use Google Analytics or PIWIK which are popular and trusted analytics solutions on the web for helping us to understand how you use the site and ways that we can improve your experience. These cookies may track things such as how long you spend on the site and the pages that you visit so we can continue to produce engaging content.

24. For more information on Google Analytics cookies, see the official Google Analytics page.