Bader Security Operating Procedures (SyOPs)

Introduction

1. This document constitutes the Security Operating Procedures (SyOPs) for the Bader application. They are issued by the System Security Officer (SSO) in accordance with MOD Departmental Security Regulations, and have been approved by the DSAS Accreditor, Acc2b. All personnel using the application 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. All users are required to tick the SyOPs checkbox on the front page of the application at logon. By ticking this box Users have explicitly agreed to comply with the security instructions detailed in these SyOPs.
2. Disciplinary action may be taken against those personnel who breach or ignore these orders. Any incident that has, or is likely, to compromise the security of the Bader application is to be reported immediately to a Bader administrator.

Scope

Role and Description of the System

3. Project Bader is the Air Cadet Organisations information management system. It is the principle cadet information management system. It is a suite of applications; Sqn Management System, Email, SharePoint, Reporting Services and e-Learning which is intended as the way in which ACO staff, VRT Officers and Volunteer Adult Staff, can best, administer ACO business through electronic Ways of Working. It replaces all Sqn legacy systems and provides a single, common, managed application which is monitored by Application Administrators.

Protective Marking

Level of Protective Marking

4. Bader stores and processes information at the PROTECT level; however, it does contain personal information and therefore warrants additional protection to comply with the legal requirements of the Data Protection Act 1998.

Responsibilities

5. Bader User security responsibilities are described in these SyOPs.

Personnel Security

Security Clearance Level & Access

6. All Bader SMS Users are cleared to, as a minimum, Enhanced Criminal Records Background Check (ECRB), access to Bader will not be granted until such time as ECRB checks are carried out.
7. Users will not be granted access to Bader SMS until they have read, understood and undertaken to comply with these SyOPs.

Computer Misuse

8. All Bader users are to comply with the MOD's Acceptable Use Policy, JSP 740. In summary Users are not to:
   a. Attempt to access areas where they are not authorised to access.
   b. Attempt to damage the application to prevent its use.
   c. Make unauthorised modifications of the application or the information contained within it.

Password Policy

9. Users who do not have an individual account have to go through a secondary sign on process and are personally responsible for the safe custody of their own passwords. Individual accounts have a single sign on and are also responsible for the safe custody of their own passwords. Under no circumstances are passwords to be recorded where they may be visible to unauthorised personnel. To ensure a minimum level of security Bader passwords are technically enforced as follows:
   a. Passwords MUST be a minimum of 8 characters in length;
   b. User created passwords MUST contain at least 1 alpha and 1 numeric and both Upper and Lower case characters;
   c. Password reset MUST NOT exceed 90 days;
   d. Passwords MUST NOT be the same as the previous 3 passwords;
   e. The user MUST be locked out after three failed login attempts;
   f. On password reset the User MUST change it at next login.

10. Users must not use easily guessable passwords; dates; family names; car registrations; organisation names; telephone numbers; Operator id; name or job related title; any other guessable personal characteristics(e.g.) address, nickname etc; and no more than two consecutive identical characters.

Storage and Media Management

Media Handling and Marking

11. Export of Bader data is permitted ONLY where a business requirement exists in order to carry out Cadet Organisation's administration; however, the following must be adhered to:
    a. Protectively marked information (PROTECT and above) saved to removable media must be encrypted with an approved product, see product options in Defence Information Assurance Notice (DIAN) 15.

Disposal and Destruction of Media

12. Data storage media no longer required must be disposed or destroyed by an approved method; see HMG Infosec Standard No.5, [IS5]. Advice on approved methods of destruction of specific types of data storage media should be sought from the ITSO/SSO.

Information Import & Export

13. The import and export of Bader data must only be carried out where a justifiable business requirement exists. All import/exports of Bader data will be audited and justification for the export will be sought by the Bader Administrator.

Acceptable Use & Monitoring

14. Bader application Users are not to tamper with the security settings or attempt to access information for which they are not authorised to view. Use of the application 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.
15. Care is to be taken to ensure Bader information is not overseen by visitors, bystanders or other un-cleared staff.
16. Bader information is not to be accessed from untrusted internet connections i.e. Internet Cafes outside of MOD establishments.

Incident Management & Reporting Security Breaches

17. Users have a duty to report security issues. In particular users are to be vigilant for actual or potential security breaches, which could include:
    a. Compromise of user passwords;
    b. Corruption of information;
    c. Non-availability of information;
    d. Loss or compromise of information.

18. All potential or actual breaches of security are to be reported to a Bader administrator they will in turn inform the DCBM, JSF, System Security Officer and Security Assurance Coordinator (SAC). The SAC is responsible for informing the DSAS Accreditor and the chain of command in accordance with JSP 541.

Privacy and Electronic Communications Regulations (2011)

19. This privacy and cookie statement covers the Bader suite at http://www.bader.mod.uk and it's subsites at domain …bader.mod.uk. Where services are delivered on the internet, this sometimes involves placing small amounts of information on your device, for example, computer or mobile phone. These include small files known as cookies. They cannot be used to identify you personally. These pieces of information are used to improve services for you through, for example:
    a. enabling a service to recognise your device so you don't have to give the same information several times during one task
    b. recognising that you may already have given a username and password so you don't need to do it for every web page requested
    c. measuring how many people are using services, so they can be made easier to use and there's enough capacity to ensure they are fast

20. You can manage these small files yourself and learn more about them through Internet browser cookies - what they are and how to manage them

Our use of cookies

Cookies for enabling the provision of services

Our website sets a cookie that stores a unique identifier for your session: We do not have any persistent cookies or any tracking/advertising cookies. If you refuse or block cookies access to Bader will be denied.

Name: ASP.NET_SessionId
Typical content: randomly generated alpha-numeric value
Expires: 20 minutes after last action

Name: smsAuth
Typical content: randomly generated alpha-numeric value
Expires: 20 minutes after last action

Name: ASPXROLES
Typical content: randomly generated alpha-numeric value
Expires: 20 minutes after last action

Name: UltiLearnLogin
Typical content: randomly generated alpha-numeric value
Expires: 20 minutes after last action

Name: WSS_KeepSessionAuthenticated
Typical content: 443
Expires: 20 minutes after last action

Name: SupportCookies
Typical content: True
Expires: At end of Session

Name: cadets_default_cadetlistview_sortorder
Typical content: sortExpression=DateOfBirthAsDate&sortDirection=0
Expires: 1 hour after creation

Name: activities_default_activitieslistview_sortorder
Typical content: sortExpression=Category&sortDirection=0
Expires: 1 hour after creation

Name: staff_default_stafflistview_sortorder
Typical content: sortExpression=FamilyName&sortDirection=1
Expires: 1 hour after creation

More information can be found at ASP.NET Cookies overview

Other websites linked from this site do not necessarily follow the same policies.

The Ministry of Defence will process personal information provided by you in accordance with the Data Protection Act 1998, for the purposes of processing enquiries, collection of statistical and associated data, and related matters.The Corporate Internet Feedback Retention Policy establishes the length of time records submitted through the 'Contact Us' email forms on the website are retained .

Further information on your rights under the Data Protection Act 1998 can be found on the Information Commissioner's website.j