ROYAL AIR FORCE AIR CADETS
PROJECT BADER
SMS | SharePoint | Learning | Mail

BADER Security Operating Procedures (SyOPs)

Issued 13th March 2017

Introduction

This document constitutes the Security Operating Procedures (SyOPs) for the all BADER applications (BADER). They are issued by the System Security Officer (SSO) in accordance with MOD Departmental Security Regulations, and have been approved by the DSAS Accreditor, Acc-Tm2-4.

All personnel using BADER 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.

By logging on to BADER Users have explicitly agreed to comply with the security instructions detailed in these SyOPs.

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 BADER is to be reported immediately to the BADER Helpdesk 030 6770 4905 for onward transmission to the BADER SSO.

Scope

Role and Description of the System

Project BADER is the Air Cadet Organisations information management system. It is the principle cadet information management system. It is a suite of applications; Squadron Management System (SMS), 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 the HQAC BADER Team.

Protective Marking

Level of Protective Marking

Bader stores and processes information at the OFFICIAL-SENSITIVE PERSONAL 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

Bader User security responsibilities are described in these SyOPs.

Personnel Security

Security Clearance Level & Access

All BADER Users are cleared to, as a minimum, Baseline Personnel Security Standard (BPSS), access to Bader will not be granted until such time as BPSS checks are carried out.

Password Policy

All personnel are personally 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.

Users who do not have an individual account have to go through a secondary sign on process when accessing SMS in order than all actions undertaken on SMS can be attributed to a named individual.

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 WILL be locked out after three failed login attempts;
f. On password reset the User MUST change it at next login.

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 such as address, nickname etc; and no more than two consecutive identical characters.

With the exception of Squadron Generic Accounts users are NOT to share their account with any other user or access an account not assigned to them without the written authority of the SSO.

Storage and Media Management

Media Handling and Marking

Export of BADER data is permitted ONLY where a business requirement exists in order to carry out Air Cadet Organisation administration; however, the following must be adhered to:

Protectively marked information (OFFICIAL 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

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 SSO via the BADER Helpdesk 030 6770 4905.

Information Import & Export

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 SSO.

Acceptable Use & Monitoring

BADER 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. BADER Users are advised that system logs are checked on a regular basis in order to detect unauthorised or suspicious system and security events.

Care is to be taken to ensure BADER information is not overseen by visitors, bystanders or other un-cleared staff.

BADER information is not to be accessed from untrusted internet connections i.e. Internet Cafes.

Incident Management & Reporting Security Breaches

BADER 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

All potential or actual breaches of security are to be reported to the BADER Helpdesk 030 6770 4905 they will in turn inform the BADER SSO who will inform the AIS 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.