DSTL ON MODCLOUD HOSTING ENVIRONMENT AND SOFTWARE AS A SERVICES (SaaS) SECURITY OPERATING PROCEDURES (SyOPs)

28 May 2024

Contents

Document Amendment Version History

Version	Date	Detail	By
	13/09/21	Merging of MODCloud SyOps into single doc. Sandbox, Dev, Prod/PreProd and SaaS ASD	Mick Murphy
0.1	28/05/24	Merging of MODCloud SyOps with Dstl requirements and specifics	Paul Cantle
0.2	12/06/24	Additional changes following Dstl and MOD review; standardised use of roles in definition of responsibilities	Paul Cantle

Annual Document Review History

Revision date	Reviewer	Owner
	David Hawke, Owen Gibbon, Dan Mulliss	Neal Hills

Acronyms / Glossary of Terms

DEFCON	Defence Contact Condition
JSP	Joint Service Publication
JSyCC	Joint Security Coordination Centre
NCSC	National Cyber Security Centre
SaaS	Software as a Service
SyOPs	Security Operating Procedures
VPN	Virtual Private Network
WARP	Warning, Advice and Reporting Point
CSE+	Cyber Security Essentials Plus
EUD	End User Device
Environment Responsible Owner	The Dstl user who is responsible and accountable for the compliance of the Environment and their Environment Users with these SyOps
Environment User	Any Dstl or third party user provided access to MOD Cloud

Scope

1. This document relates to all services and environments offered by Dstl, delivered via MOD's Core Enabling Services Team and consumed by Dstl and their partners. The Hosting Environment will be referred to as "the Environment" and MODCloud provided Software as a Service as "SaaS". The Controls defined in these SyOPs, are to be implemented and adhered to to assure the use of The Environment and consumption of SaaS conforms with MOD and Dstl security policy.

2. These SyOPs are intended for all Environment Users who require use of MODCloud Official hosting. All Environment Users must also read and comply with any applicable SyOPs / Security Instructions (SyIs) for each of the End User Devices (EUD) that are used to access The Environment.

3. The MODCloud Environment User is expected to understand, implement, and adhere to these SyOps. The understanding and agreement being acknowledged by either responding to email sent by MODCloud Admin that contained the SyOPs or by accepting the check box within JSM during onboarding. Dstl authorities will review and amend these SyOps as required and upon change Environment Users will be requested to review and resign the declaration.

4. Whilst these SyOps consider the baseline requirements for MODCloud they may not extend far enough to mitigate all procedural controls required by the Environment Responsible Owner when considering their own Risks and data sets. The Environment Responsible Owner may reinforce these SyOps to meet their own requirements but may not in any way degrade these baseline MODCloud controls. Environment Users are expected to ensure their own customers understand and adhere to these SyOps.

System Description

5. Sandbox, Development, Test, Pre-Production and Production are the names afforded to MODCloud customer subscriptions to enable a clear distinction of their purpose in the development

pipeline. At each stage specific, Accreditation and Authority to operate requirements must be met by the Environment Responsible Owner. The following paragraphs briefly describe the purpose of each type of use and the governance requirements:

a. **MODCloud Sandbox Account**. A sandbox account is enabled upon request to facilitate proof of concept work and experimentation. Environment Users must be aware that due to the intended purpose of this account **NO** MOD or Personal Identifiable data is to be used within these accounts. Additionally, Sandbox accounts are **NOT** permitted to be connected, in any way, to MOD or HMG services including MODNet EUDs. Any work that involves the Environment User contravening these requirements will require the Environment Users to comply with the JSP 604 ruleset and MOD Data protection policies, requiring 604 case officer and accreditor involvement. If this is the intention of the Environment User it is suggested that they approach MODCloud for a Development account.

SANDBOX Account

NO MOD or PERSONAL Identifiable data.

NO connection to other MOD or HMG systems.

NO requirement for JSP 604 or JSP 440 authority.

b. **MODCloud Development & Test (Dev/Test)** accounts provide System, service and Application Owners, areas to install, develop, test and administer Applications and Services on MODCloud up to and including System and Acceptance testing prior to deployment to Pre-Production and Production. Usage of Dev/Test is subject to JSP 604 (Network Joining Rules) ruleset and JSP 440 as determined by the designated Case Officer and Accreditor. The Environment Responsible Owner is the responsible for the separation and segregation of the Dev and Test activities within the environment. Application of NCSC Cloud Security principles[1] is expected.

Dev/Test Accounts

Subject to Customer lead JSP604 and 440 authority but may only require documented agreement or authority to test (ATT) authority from Governance authorities.

c. **MODCloud Pre-production and Production Environments (Prod/Pre-Prod)**, permits Environment Users to verify, deploy administer and operate their services within the MODCloud environment. Access to MOD networks is permitted therefore Environment Users **MUST** be aware it is the responsibility to ensure compliance with JSP 604 and 440. Authority to operate and accreditation must be demonstrated. Application of NCSC Cloud Security principles[1] is expected.

[1] https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

Pre-Production and Production
Subject to Customer lead JSP604 and 440 authority. Interim or full Accreditation and proof of IATO or ATO must be provided to MODCloud.

d. **MODCloud SaaS,** is intended to provide multiple MODCloud customers, with similar service and software requirements, a cloud-based solution thus reducing MOD replication and overburden of services and management overheads. MODCloud SaaS offerings include, but are not limited to:

(1) Atlassian Jira
(2) Atlassian Confluence
(3) Microsoft SharePoint
(4) GitHub

Purpose

6. There are two complimentary means by which information risk is mitigated as much as is possible:

a. **Technical Controls** – These are generally technological components which combine to provide security functionality that protects a business process.

b. **Procedural Controls** – These are generally process or instructional in nature and serve to perform risk mitigation where a technical control cannot be (or is not) in place.

7. These SyOPs serve to mitigate certain inherent risks which cannot be fully covered by a technical control or whereby the implementation of a control is not practicable or commensurate with the risk reduction. All Environment Users are required to be aware and able to operate within the Government Security Classification scheme.

8. Use of MODCloud Environments and SaaS offering is conditional on Environment Users abiding with these SyOps. Any action which breaches these SyOps could result in the Environment User's access being withdrawn.

Once an Environment User has read this documentation, they MUST confirm in writing to modcloud_admin@dstl.gov.uk, indicating they acknowledge, will abide by, and implement, within their area of responsibility, the rules stated with this document. If this SyOPs has been read as part of an onboarding form, then selecting the tick box to confirm adherence is acceptable.

Classification

9. The highest Classification of information that The Environment is assured to process and/or store is OFFICIAL, this includes data CAVEATED as OFFICIAL-SENSITIVE (OS).

a. Where **OFFICIAL-SENSITIVE**, including caveats, is consumed by an Environment User the Environment Responsible Owner **MUST** ensure that suitable measures are in place and appropriate accreditation has been sought.

9. Where an Environment User has a requirement to process Personal data within the Environment, it is the responsibility of the of data owner to ensure that the relevant Data Protection Impact Assessment (DPIA) has been undertaken and endorsed. The current DIN 2018DIN05-14 refers. If superseded comply with current.

10. Where an Environment User has the requirement to process any Bulk Data in the Environment, it is the responsibility of the Environment Responsible Owner to ensure that the relevant Bulk Data Assessment has been undertaken in accordance with 2018DIN02-004. If this DIN is superseded comply with current.

11. Where information relating to the International Traffic Arms Regulation (ITAR) is used, the Environment Responsible Owner MUST have suitable documentation and controls in place. DIN 2017DIN04-101 refers.

NSV and Contractual Requirements

13. The Environment Responsible Owner must ensure that all privileged Environment Users (a system account which has administrative privileges) hold a valid Security Vetting Status of SC, as defined in JSP 440 leaflet 7and DEFCON 76. Additionally in accordance with JSP 440 leaflet 7 para's 7 and 12, all Environment Users (any individual with access to MOD Information) of MODCloud are to hold a minimum vetting status of UK Baseline Personnel Security Standard (BPSS).

14. Environment Users utilising 3rd party suppliers must ensure they appropriately comply with JSP 440 Leaflet 13. All MOD Contracts must, as a minimum, comply with:

a. DEFCON 531 (Disclosure of Information)
b. DEFCON 532A (Protection of Personal Information (Where Personal Data is not being processed on behalf of the Authority)) or DEFCON 532B (Protection of Personal Data (Where Personal Data is being processed on behalf of the Authority)).
c. DEFCON 76 (Contractors at Government Establishments)
d. DEFCON 659 (Security Measures)
e. DEFSTAN 05-138
f. The EUDs or connected devices to be in scope of supplier NCSC Cyber Essentials Plus[2]

Software and Data

15. All data and software **MUST** be from authorised sources and be assessed for suitability for use within the environment by MODCloud and for use by the Environment Users themselves. It is the Environment Users' and/or Application Owners' responsibility to ensure all software in use is appropriately licensed and with the latest security patches.

[2] https://www.ncsc.gov.uk/cyberessentials/overview

16. Environment Users **MUST** note that it is expected wherever possible to ensure that their data is stored and processed within the UK. It is the Environment Responsible Owners responsibility to ensure that they are aware of where their data is held and processed. If data is stored or transmitted outside of the UK region appropriate measures and authority is to be sought by the Environment Responsible Owner.

17. All data introduced via removable media into the Environment **MUST** be scanned with an Anti-Virus software product before being uploaded to the Environment.

18. MODCloud will ensure that all system patches are applied to the Environment in accordance with the relevant JSP 604 timescales, this includes all system components within the Environment that are managed by the Application Owner. It is the assumption that the Application Owner will patch any software that is not provided as a service by MODCloud.

Anti-malware

19. The Environment will apply appropriate Anti-Malware Policies and Anti-Malware controls the level to which they extend are dependent upon the Service Offering being consumed by the Environment User.

Accessing the service

20. Dstl's Environment Users **MUST** use Multi-Factor Authentication to access all environments.

21. Environment Users will abide by these SyOps or those written by the Environment Responsible Owner which reinforce these SyOps.

Connecting to or from other networks and services

22. Any Environment User required connection to external networks or services shall have been approved by the appropriate authority (JSP 604/440) and that the Environment User has permission to do so.

Environment User Access Devices

23. The Environment Responsible Owner is to ensure that any Environment Users accessing the environment or SaaS, MOD or Partner approved, utilise End User Devices (EUD) that hold a valid and current Security Accreditation status. If this is not the case and access is from the Environment User's own device, then the device must be in scope of an in date Cyber Essentials Plus certification [3]with the NCSC Cyber Essentials certification or equivalent. More specifically that:

a. The device has Anti-Malware software installed and that this is kept up to date
b. It is patched with the latest software and security patches on a regular basis
c. Installed software is obtained from a trusted source.
d. There is some method to limit access to authorised personnel only.
e. It is audited on a regular basis.

[3] https://www.ncsc.gov.uk/cyberessentials/overview

24. Upon leaving any EUD unattended the Environment User must lock the EUD. When closing for the day or moving to another location Environment Users **MUST** ensure they are logged of and the EUD has been shut down.

25. Environment Users **MUST** adhere to one of the following practices when accessing The Environment.

a. Access from Dstl DONB EUD via DONB network (if Environment User is not on-prem, this will be routed through VPN from EUD to DONB)
b. Access from Dstl GUEST network (any EUD i.e. Grey IT, Developer laptop, third party device; from Dstl premises)
c. Access from previously advised, agreed and suitably secured corporate network (if not directly from corporate network, then EUD must be connected via VPN to the corporate network)
d. If a device is used by a trusted partner/supplier, the partner/supplier must be CES+ and the EUD must be connected to a VPN before accessing the CCoE.

Passwords

26. Accounts are provided to Environment Users with a default password, which they must change on first use, Environment Users should follow NCSC password guidance when selecting a new password. A recommended starting point is as follows:

a The minimum password length is 9 characters. Admin or privileged accounts are to be protected by a 12-character password.

b It must contain a mix of UPPER and lower-case letters, numbers, and symbols (£, $, &, @, etc.).

c It is recommended that a password phrase such as ‘IL1v3InAH0u5eW1th@Wh!teD0or’ is used.

d It must not be easily guessable or relate to well known or readily available personal information.

27. Environment Users MUST not share their password with others. No other individuals or organisations have any requirement to know an Environment User’s password.

28. Environment Users MUST not reuse passwords from or on other systems or services.

29. Environment Users MUST not leave written passwords or reminders near the Environment User’s EUD or in areas where they will be visible to others.

30. Environment Users MUST not access The Environment using another Environment User’s login details.

31. If an Environment User suspects their password has been disclosed to anyone else, they MUST immediately change their password and notify system Point of Contact.

Monitoring

31. The environment and SaaS offering are monitored and audited to ensure that the confidentiality, integrity and availability of MOD data is maintained and to identify any potential abuse of privileges assigned to application development staff and Environment Users. All Environment Users are therefore advised that their data and activities, whilst subject to protection under the Regulation of Investigatory Powers Act and Data Protection Act, will also be subject to security monitoring and can be accessed by investigating staff in the course of their duties. The Environment Responsible Owner is to ensure that the level of monitoring provided by MODCloud is appropriate to their needs. Where a shortfall is identified the Environment Responsible Owner is responsible for ensuring compliance.

SECURITY MONITORING NOTICE

.

The Environment is routinely monitored, recorded and audited to ensure that the confidentiality, integrity and availability of MOD data is maintained and to identify any potential abuse of privileges assigned to application owner development staff. All Environment Users of The Environment are therefore advised that their data and activities, whilst subject to protection under the UK Investigatory Powers Act 2016, Data Protection Act and General Data Protection Regulation, will be subject to security monitoring and can be accessed by investigating staff in the course of their duties

Personnel Security

32. All Environment Users will be provided with SyOps appropriate to the Environment and their own role. They will acknowledge compliance with SyOps by completing a Declaration, appropriate for the Environment, prior to accessing the MODCloud environment or SaaS offering. The Environment Responsible Owner for the Environment is to acknowledge and sign these SyOps. In doing so they agree to comply and implement them and garner similar agreements from their own Environment Users.

33. Environment Users may be required to provide copies of signed SyOps/Declarations upon request.

Prohibited Use

34. The person who signs these SyOPs is responsible for disseminating the information contain within this document to all Environment Users of the service and **MUST** ensure that all Environment Users understand that they must comply with them if they wish to continue using the service.

35. MODCloud has implemented configuration and technical controls to enable accounts to be used by MODCloud customers, such as subscription name, for billing and monitoring purposes. Environment Users **MUST** not attempt to amend or manipulate preconfigured elements of these accounts. Should a requirement to amend these parameters arise a MODCloud Request for Change (RFC) should be raised. Any RFC raised will be assessed for impact to MODCloud before implementation may be endorsed.

36. Sandbox is NOT intended to be used for connection to any other MOD or HM Government system for transfer of data or other access other than for access from the internet. Environment Users must be aware that the Sandbox account and its contents have not been assessed against MOD JSP 604 or 440 and practices, which is a requirement before any interoperation or connection to another system is permitted.

37. Improper use of MOD IT or Telecoms comprises of a range of activities and behaviour, contrary to SyOPs, sound practice, common sense or UK Law, and is defined as “the deliberate, inappropriate or illegal use of any part of the MOD IT or Telecoms”.
Action may be taken against anyone who misuses MOD IT or Telecoms and may result in legal action were this is deemed appropriate.
The MOD complies with its own Acceptable Use policy the main tenants of which are outlined below, Environment Users **MUST** comply with policy to enable continued use of the service.

ACCEPTABLE USAGE POLICY NOTICE -

YOU MUST NOT KNOWINGLY USE MOD IT OR TELECOMS TO:

- **Access, store or transmit offensive, indecent or obscene material or abusive images and literature.**
- **Access, store or transmit material which can reasonably be considered as harassment of, or insulting to, others.**
- **Access, store or transmit material obtained in violation of copyright or used in breach of a licence agreement.**

- **Transmit spam (electronic junk mail) or chain email.**

- **Store or transmit material that could reasonably be expected to embarrass or compromise the MOD.**

- **Conduct commercial activities which are not connected to MOD business.**

- **Undertake any form of gaming, lottery or betting.**

- **Undertake any form of share dealing.**

- **Offer items for sale, or place bids on, commercial auction sites (such as eBay™).**

- **Participate in Chain Schemes (such as pyramid selling).**

- **Create, store or send material designed to mislead people about who originated or authorised it (e.g. through misuse of scanned signatures).**
- **Attempt to compromise MOD IT and Telecoms, prevent legitimate access to them, damage them or seek to cause degradation of performance or a denial of service.**
- **Attempt to gain unauthorised access to MOD IT and Telecoms or content for which you do not have permission (i.e. Hacking).**

- **Attempt to access, amend, damage, delete or disseminate another Environment User's files, emails, communications, or data without the appropriate authority.**

38. Environment Users should be aware that it is an offence, under the Computer Misuse Act 1990, to knowingly access a computer system or modify its contents without permission. Any person who knowingly accesses The Environment other than for an authorised purpose is therefore committing an offence and may be subject to legal action.

Incident Management

39. Any Security Incidents (such as Malware, or unauthorised configurations of virtual infrastructure, etc.). If Environment Users believe the confidentiality or integrity of the information, they are working on has been compromised (e.g. Environment has been compromised or there is indication or suspicion that it may have been tampered with etc.) they **MUST** report it immediately to the MODCloud Ops Team

40. If an Environment User notices, or suspects, any suspicious activity on the Environment, they **MUST**:

a. Stop using The Environment and the EUD being used for access immediately.

b. Report the incident to the MODCloud Ops Team and the MOD JSyCC WARP.

i. Warning Alert and Reporting Point (WARP). In order to resolve IA incidents quickly with the minimum disruption to Defence CIS, it is important that you know which is your WARP and how to contact them. The link attached provides a directory of WARP contact details WARP Contact List URL then select the top file - JSyCC Incident Contact List.

c. If Computer Network Defence (CND) incident, then report immediately to the Defence CIS Single Point of Contact (SPOC) and use the utterance “MODCERT”; the SPOC will then direct you straightaway to the MODCERT team at MOD Corsham:

i. Short Dial: 188 Military: 96 600 8 9 10 Civilian: +44 (0) 870 600 8 9 10
ii. Email Intranet: SPOC-CIS Email Internet: SPOC-CIS@MOD.UK
iii. Web: http://dcsaspoc.diif.r.mil.uk/

d. If the incident is related to Information Security, then it should be reported in the first instance to your WARP or, if the WARP cannot be contacted, to the JSyCC at MOD Corsham:

i. Military: 94 963 Ext 3743
ii. Civilian: +44 (0)1225 843743
iii. SMART Numbers:
iv. Military: 96 770 Ext 2187
v. Civilian: 030 6770 2187
vi. Duty Officer: vii. Mobile: +44 (0) 7768 558863
viii. Mail JSyCC, Building 405, MOD Corsham, Westwells Road, Corsham, Wiltshire, SN13 9NR ix. Email Intranet: CIO-DSAS-JSyCCOperations
x. Email Internet: CIO-DSAS-JSyCCOperations@MoD.uk

e. Co-operate fully with any security investigation that is being carried out by an authorised person or delegated person on behalf of the MODCloud Ops Team.

f. Take advice from the MODCloud Ops Team before powering off or deleting any virtual infrastructure components within The Environment.

g. Take advice before switching off or rebooting the EUD used to access The Environment from their local Security staff.

Any breach or contravention of these SyOPs and associated Acceptable Use Policy (AUP) may render the offender liable to administrative, disciplinary, or legal action.

References

JSP 440
JSP 604
DICyPD/2019-004
Computer Misuse Act 1990
Data Protection Act 2018
General Data Protection Regulation 2018
UK Investigatory Powers Act 2016

I confirm that I have read, understood and will abide by the MODCloud environments and SaaS SyOps and will ensure that all Environment Users of the service are aware and abide with its contents

Rank / Title	Name	Post
Signature		Date
Organisation/Unit		