# DEFENCE DEVSECOPS SERVICE (D2S) SYOPS ADDENDUM

`version 1.1`

This Addendum **SHALL** be read in conjunction with the Defence Digital Foundry SyOps.

Users of D2S, in addition to following the requirements of the Defence Digital Foundry SyOps **SHALL** additionally abide by the following:

- **Responsible person:** Each development team **SHALL** have a responsible official/officer; this person **SHALL** be a Crown servant with seniority not less than OF3/Chief Inspector/Senior Executive Officer (formerly C1). This person **SHALL** be accountable to Defence Digital for ensuring the activities of the team overall adhere to the SyOps. Each user **MUST** know who their responsible official/officer is.
- **Classification:** D2S' OFFICIAL environments are intended for creating assets with a classification of OFFICIAL (including all caveats) such as source code, comments, markdown files. Users are responsible for ensuring that assets they create or manage using the OFFICIAL environments **MUST NOT** have a classification of SECRET or above, based on the Government Security Classifications policy. *Note: the classification of code will often be different than the classification of the information it is used to process.*
- Devices used to consume D2S **MUST** be controlled devices, following the controls specified in Section 2 of the Defence Digital Foundry SyOps.
- These devices **SHOULD** follow the Device Security Guidance and use a suitably configured Mobile Device Management system.

## Source Code Management

- **Sharing**: Users are reminded of the Civil Service Code's obligation to "handle information as openly as possible within the legal framework" and that all MOD users are expected to abide by the Code. In particular, users are reminded that source code is a Crown asset: users **MUST** not keep assets from other teams unless there is a specific and compelling reason to enforce a 'need to know' restriction. Teams **SHOULD** construct their assets in such a way as to maximise reuse opportunities, in particular by applying the Security considerations when coding in the open guidance and avoiding intellectual property barriers.
- **Review**: When providing or receiving feedback on code, users **SHOULD** respect and value alternative viewpoints and seek, accept and offer honest criticisms of work as required by the Chartered Institute for IT's code of conduct.
- **GitHub**: The following GitHub standards **SHALL** be followed by all teams:
    - All repos are to be set as private or internal
    - All commits to a release branch must be signed
    - Have main as the default branch
    - Delete branch on merge
    - Have non-empty description (shouldn't be null or "")
    - Have issues enabled
    - Have recent activity (pushedAt < ?)
    - Checks for stored credentials is undertaken prior to commit
    - Have branch protection on main, with:
        - Require a pull request before merging
        - Require approvals option and a nominated person to approve the pull request
        - Require review from Code Owners option
        - Include administrators option
        - have Dependabot enabled

## For Development Environments:

- D2S development environments **SHALL ONLY** be used for development and prototyping work only. Development includes all D2S activities short of integration testing with services or systems in another environment or running production workloads. This may include creating and carrying out unit testing, test automation, code creation, code compilation, alpha prototypes and performance benchmarking within the assigned namespace(s). For the avoidance of doubt integration tests and production workloads **SHALL NOT** be permitted in development environments.
- Work in development environments **MUST** use synthetic test data unless approval has been obtained from appropriate person(s) to do otherwise. Synthetic test data means test records that do not reflect any genuine MOD activity or entities (only the schemata and data formats may be genuine). Because of the difficulty of achieving true anonymisation, test data **SHOULD** be generated through a process other than anonymisation of genuine data.

## Integration Testing & Production Services:

- Users **SHALL** be responsible for satisfying all JSP604 rules, unless explicitly advised that a rule has been satisfied or an exemption has been obtained on their behalf by another party (e.g. via D2S assurance inheritance). Unless advised otherwise, users **SHALL** be responsible for ensuring required approval from the Release and Deployment Board is obtained prior to integration testing with other services or providing a production service. This activity **SHOULD** be started as early as possible, during the development process.
- Production workloads **SHOULD** be run in a namespace designated for that purpose (i.e. not in a development namespace).

  *For the avoidance of doubt, any workload used to conduct or transact real Defence business or process genuine Defence information constitutes a production workload (regardless of the intended purpose of the environment in which the workload is running). Production is sometimes described with the term 'live'. For the avoidance of confusion this is not the same as 'live' in the meaning of the Government Service Manual. Services in the private beta, public beta or live service phases as set out in the Manual are all considered to be 'production' services.*