Defence Digital Foundry

User Security Operating Procedures (SyOPs)

Introduction

This document constitutes the User Security Operating Procedures ("SyOPs") for the Defence Digital Foundry ("Foundry") and the devices and services (including Cloud Software as a Service "SaaS" tools) that the Foundry provides.

Security is everyone's responsibility. All of us need to take steps to help keep Ministry of Defence ("MoD") information and systems secure. This document sets out some of the key things we need to do.

This is a Google Docs document that lives in the "Shared" Drive. Link Here. All users with a Foundry Identity (@digital.mod.uk) have access to this drive and document. It is also published to GitHub - https://github.com/defencedigital/foundry-syops with version history. Any updates to this document will be announced in the Foundry Slack and an email to all active users.

The use of Foundry devices and services implies implicit agreement with this document and the acceptable use policies and code of conduct.

Official Secrets Acts

We are all subject to the provisions of the Official Secrets Acts 1911-1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular.

We all continue to be subject to the Act beyond the end of our employment or contract.

Document Structure

The following outlines the document structure:

Introduction: Presents the purpose of the SyOPs, and general information.

Section 1: Presents the acceptable use policies and the code of conduct which includes references to the civil service code.

Section 2: Defines the activities and use of the system that are prohibited for any user whilst using Foundry devices and services.

Section 3: Provides high-level detail as to the incident response process in relation to Foundry services. Points of contact are listed in the event of a security incident.

System Overview

The Defence Digital Foundry operates a range of systems to support defence activities as set out in the Digital Strategy for Defence. This includes but is not limited to:

- Identity and Cloud Services
- Device Management enabling MoD issued Computers for use with Foundry services.
- Software Development services and hosting platforms.
- Cloud SaaS tools to support Digital Teams create and deliver Digital Services and Products.

Defence Digital Foundry systems and services are for a wide range of use cases to allow digital teams to create services and products quickly. There are four types of use case that are to be catered for in this SyOPs:

1. MoD Users (Civilian and Military) using MoD/Foundry issued equipment.
2. MoD Users (Civilian and Military) using personal equipment.
3. MoD Suppliers using MoD/Foundry issued equipment
4. MoD Suppliers using Supplier issued equipment.

The purpose for these four distinct use scenarios allows for flexibility in access to cloud services, especially in urgent situations. This only applies to OFFICIAL (including caveats such as SENSITIVE) information. SECRET and TOP SECRET information and systems are not covered by this SyOPs.

Classification

The classification for all Internet connected Defence Digital Foundry systems and services are OFFICIAL. OFFICIAL systems can carry documents with the SENSITIVE caveat as per HM Government Security Classification policy.

SECRET and TOP SECRET systems and services will be managed with supplemental acceptable use policies and codes of conduct. Any information that is protectively marked above OFFICIAL must not be accessed, processed or stored on OFFICIAL services or devices.

All documents that are classified OFFICIAL do not need to be marked as per the guidance for working with OFFICIAL information. However where the document or information is SENSITIVE the document needs to be clearly marked. Please ensure that you have read the guidance for working with OFFICIAL information.

Government Security Clearance

All Users of Foundry Services must hold a Government Security Clearance of at least BPSS. Projects and services may require higher clearance levels depending on the project and data being processed by that project or service.

Section 1 - Policies and Code of Conduct

Acceptable Use Policy - JSP 740 Part 1

The Acceptable Use Policy is derived from JSP 740 Part 1 - v5.0 is published online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1062407/JSP740_Part1.pdf

When and where does the Acceptable Use Policy apply?

- The MOD provides Information and Communications Technology ("ICT") and services for Defence-related activities of all kinds, including normal work, training, and official trade union business. Limited personal use is also permitted. Whenever you use ICT and services owned or operated by the MoD, you must do so responsibly.
- This Acceptable Use Policy ("AUP") applies to everyone (military and civilian) at all times when using the MoD's ICT and services. It also applies if you are on detached duty, and using ICT and services supplied by another authority for your work for Defence, or are a contractor or occasional user of MoD ICT and services.
- You must abide by this AUP, as well as the Security Operating Procedures (SyOPs) for the equipment you're using. You must also follow the Defence Security Handbook, the MoD Corporate Standards Guide and your Service Code of Conduct at all times.

Prohibited activities whenever using MoD ICT and services

You must not knowingly:

- Offend, insult, harass, threaten or deceive other people.
- Request, create, access, store or send offensive, pornographic, indecent or illegal material.
- Breach copyright or licence agreements.
- Connect unauthorised devices to MoD ICT or networks.
- Connect MoD mobile devices to unauthorised computers.

- Download, use, store or distribute software or applications that are unauthorised or not accredited for the system you are using.
- Configure email to auto-forward or create rules to bulk-forward mail to non-MoD email addresses.
- Remove, disable or nullify operational components, safety or security measures in MoD ICT.
- Try to misuse, gain unauthorised access to, or prevent legitimate access to, any ICT equipment, network, system, service or account.
- Try to gain unauthorised access to information, or release information without proper authority.
- Bring the MoD into disrepute or obstruct its business.

- Be negligent in protecting the ICT and services, or the information you can access from it.
- Break the law, unless your role has been authorised as one where a specific exemption stipulated in current legislation has been applied.
- Encourage others to break the law.

Personal use of MoD ICT

The MoD allows you limited personal use of its ICT (although this can be stopped at any time at the MoD's discretion). You are permitted to make personal purchases from websites (except auction sites). Where this activity requires a username/password combination, the details provided must not contain any MoD-specific information.

When making personal use of MoD ICT, you must not:

- Take part in personal commercial activity, including, but not limited to, peer-to-peer marketing.
- Undertake any form of share-dealing.
- Take part in any gambling or lottery (except that you may participate in one of the four lotteries run by Defence to support sporting facilities – the RN & RM, the Army, and the RAF Sports Lotteries, and the MoD Lottery).
- Take part in petitions, campaigns, politics or similar activity.
- Waste MoD time, money or resources.
- Use any MoD email address to sign up to public websites or services.

The MOD does not accept any liability for any loss, damage or inconvenience you may suffer as a result of personal use of its ICT and services. The MoD monitors its networks, so if you don't want it to see your private information, only use its ICT for work.

Civil Service Code & Contributor Covenant Code of Conduct

Contributors to repositories hosted in the Defence Digital Foundry are expected to follow the Contributor Covenant Code of Conduct, and those working within Government are also expected to follow the Civil Service Code.

Note:

- *where the code of conduct says "project" we mean the Digital Foundry, `defencedigital` and 'ministryofdefence' and all repositories hosted within it.*
- *where the code of conduct says "maintainer" we mean `Defence Digital Foundry` organisation owners*
- *where the code of conduct says "leadership" we mean both `Defence Digital Foundry` organisation owners, line managers, and other leadership within Defence Digital Foundry.*

Our Pledge

In the interest of fostering an open and welcoming environment, we as contributors and maintainers pledge to making participation in our project and our community a harassment-free experience for everyone, regardless of age, body size, disability, ethnicity, gender identity and expression, level of experience, nationality, personal appearance, race, religion, or sexual identity and orientation.

Our Standards

Examples of behaviour that contributes to creating a positive environment include:

- Using welcoming and inclusive language
- Being respectful of differing viewpoints and experiences
- Gracefully accepting constructive criticism
- Focusing on what is best for the community
- Showing empathy towards other community members

Examples of unacceptable behaviour by participants include:

- The use of sexualized language or imagery and unwelcome sexual attention or advances
- Trolling, insulting/derogatory comments, and personal or political attacks
- Public or private harassment
- Publishing others' private information, such as a physical or electronic address, without explicit permission
- Other conduct which could reasonably be considered inappropriate in a professional setting

Our Responsibilities

Project maintainers are responsible for clarifying the standards of acceptable behaviour and are expected to take appropriate and fair corrective action in response to any instances of unacceptable behaviour.

Project maintainers have the right and responsibility to remove, edit, or reject comments, commits, code, wiki edits, issues, and other contributions that are not aligned to this Code of Conduct, or to ban temporarily or permanently any contributor for other behaviours that they deem inappropriate, threatening, offensive, or harmful.

Scope

This Code of Conduct applies both within project spaces and in public spaces when an individual is representing the project or its community. Examples of representing a project or community include using an official project e-mail address, posting via an official social media account, or acting as an appointed representative at an online or offline event. Representation of a project may be further defined and clarified by project maintainers.

Enforcement

Instances of abusive, harassing, or otherwise unacceptable behaviour may be reported by contacting the project team at code-of-conduct@digital.mod.uk

All complaints will be reviewed and investigated and will result in a response that is deemed necessary and appropriate to the circumstances. The project team is obligated to maintain confidentiality with regard to the reporter of an incident. Further details of specific enforcement policies may be posted separately.

Project maintainers who do not follow or enforce the Code of Conduct in good faith may face temporary or permanent repercussions as determined by other members of the project's leadership.

Attribution

This Code of Conduct is adapted from the Contributor Covenant, version 1.4, available at https://www.contributor-covenant.org/version/1/4/code-of-conduct.html

Section 2 - Personal/Supplier Device Use

If you're setting up a non-MoD device for MoD work then there are a few steps you need to take:

1. It needs to be a modern device running the latest version of a major operating system.

2. Automatic security updates need to be enabled, and you need to allow them to be installed promptly when they become available.

3. Your device needs to have encryption enabled for data at rest. Using the manufacturer's native encryption is fine.

4. To decrypt or unlock the device will need to enter a password. If it's a laptop we recommend three random words. For a mobile device you can use a shorter pin and biometrics.

5. For other passwords we recommend you consider using a password manager. 2-factor authentication should also be used wherever possible, but definitely for your G Suite and Slack accounts.

6. If you back up data, make sure it's encrypted. Ideally your work should be stored in G Suite so it's automatically backed up.

7. On a laptop you should consider anti-virus software. Ask #digital-foundry on slack for advice on suitable products. Another good step is to use a DNS service that filters malicious domains (9.9.9.9 is a good example).

8. If your device is left unattended for a few mins, it should be configured to lock automatically.

9. You should not share the machine with anybody else (e.g. other members of your family).

You shouldn't leave your laptop unattended in a public place, a motor vehicle boot or luggage compartment at any time. If you use a hardware token (eg yubikey) ensure it is not stored with the machine.

Section 3 - Security Incident Reporting

All users are responsible for reporting any unusual, suspected or actual security incidents immediately to the Digital Foundry, Information Owner or relevant Security Team.

Failure to report any incident may jeopardise any investigation or other follow-up or remedial action later discovered to be necessary. In the event of any security vulnerabilities or breaches of the current security regulations being identified the following actions are to be taken:

- Secure the device in question by disconnecting it or turning it off.
- Secure any relevant supporting evidence e.g. removable media (if applicable).
- List anything relevant to assist in any investigation.

During normal working hours make an immediate report to the appropriate team

Reporting Channels

MoD Users (Civilian and Military): The Digital Foundry:

- the **#help** channel of the **https://defencedigital.slack.com** slack workspace
- email security@digital.mod.uk

Front Line Commands, the relevant Security Team or Information Owner in addition to the Digital Foundry above.

Suppliers, your local Security Team **and** the Defence Digital Foundry

Faults, Defects and Potential Vulnerabilities

Upon discovery of faults, defects and potential vulnerabilities affecting Foundry devices or services, please use the same reporting channels above and supply as much information as possible to support the investigation.

Section 4 - Software & Service Usage

Using software and services, including cloud 'Software as a Service' tools please keep to the following behaviours

Logging into Software / Services

The Defence Digital Foundry will endeavour to integrate software and services with a single Identity that is provided as part of the onboarding process and will control access to relevant services through the Identity. Please ensure that:

- When you sign into services, you are aware that the website you are signing into has a valid certificate/padlock to verify the website's identity.
- When using a piece of software or service that is integrated with the Foundry Identity, you shouldn't need to enter your password again if you can "Login with Google". If you are requested to login again ensure that you are logging into the Google Identity portal and not a generic set of credentials fields.

Your Google Identity may allow you to sign into other services not provided by or paid for by the Foundry. Please use discretion to only sign into services you need to do your role.

Password Security & Multi-Factor

Foundry Identity based on the @digital.mod.uk email address will require multi-factor authentication after you have signed in for the first time. This can be either a physical token such as a Yubi-Key, a soft-token that uses something like the Google Authenticator or push to app feature for confirming activities.

Files & Sharing

Foundry provides Google Drive and GitHub for creating, collaborating and storing information. Shared Drives are managed by the Foundry and are owned by the Drive Admins for that area. GitHub repositories are owned by the team that create them and can have different visibilities: Public, Internal or Private.

Please take care when sharing files with external groups. Controls are in place to prevent public sharing.

Do not export files to send as attachments if the person or team you are working with are not on the allowed list of domains unless you have permission from the data owner.

Google Drive

Personal files in “My Drive” are owned by you. They can be shared with anyone in the organisation or in the organisation’s allow list of external domains.

All projects or related shared files should be created in Shared Drives that are relevant to your project or team. The drive admin for that drive can control access to the drive.

If an individual requests access to a specific file in Google Drive, you will receive an email notification of the request. Please be careful when clicking links to share files and ensure you are aware of the request from the individual making the request via other methods such as Slack.

GitHub

Individuals who are using GitHub should be familiar with the different types of visibilities that are available for repositories.When collaborating with content, code or other data in GitHub, please ensure you follow the Contributor Covenant Code of Conduct as outlined above.

When repositories are created, they must be created in the organisation, such as **github.com/defencedigital**

Public repositories are visible to the Internet. It is important to ensure that public repositories are operated correctly and do not expose the internal working of the Ministry of Defence.

Internal repositories are visible to everyone in the organisation, not the Internet.

Private repositories are only visible to the team or individuals that the repositories are shared with directly and not the Internet.

Other SaaS Tools

In addition to the core services of Google and GitHub, all the other tools benefit from a considered approach when using the tools. The SaaS tools that are available are there to make the work you are contributing to easier to manage and track and organise.

- When using SaaS tools, ensure you are signed in with your @digital.mod.uk Google Identity. It helps to use Chrome which is signed into the Google Identity to simplify signing into other Foundry services.

- When creating or editing content on SaaS tools, ensure that the content is OFFICIAL (including caveats) and when sharing that content it’s only shared with the relevant people who need to have access to it.