ONS Source Code Management Policy
Source Code Management Acceptable Use Policy

Implemented on (date)	20/05/2024
Approved by (name & role)	Head of Software Practices (Fahad Anwar) In consultation with TAG (Technical Advisory Group)
Last review on (date)	16/05/2024
Reviewed by	TAG (Technical Advisory Group)
Next review due on (date)	16/05/2025
Policy owner (name)	Head of Software Practices In consultation with Technical Advisory Group (TAG) representing Software Engineers, Cloud Division, TISS and Security Division.
Policy owner (division)	Digital Services and Technology (DST)
Main point of contact (name)	Fahad Anwar Software Engineering Head of Practice
Status	Approved

Policy Review Record

This Review Record is to be completed on each time a review is conducted. Its purpose is to maintain a record of reviews, recording who conducted the review (policy owner), the date of the review and the outcome of the review (policy fit for purpose, amendment required, policy no longer required, etc).

This Policy is to be reviewed annually.

Review No	Review Conducted By	Review Date	Review Outcome
01			

Amendment Details

Date	Amendment Summary	Amended by	Version

RASCI (For detail please – RASCI Information document)

Responsible	G6 Program Managers
Accountable	Head of Software Practices
Supportive	Head of Cloud Functions (Amazon, GCP, Azure) SAIM SIRA Software Engineering Community of Practice (SE-CoP)
Consulted	Technical Advisory Group (TAG) representing Software Engineers, Cloud Division, TISS and Security Division.
Informed	Senior Leadership Team Software Engineering Community SAIM SIRA Design Authority Chair

Source Code Management Acceptable Use Policy

Scope
Digital Services and Technology and any external parties delivering services into DST (unless by agreement).

Background
Source Code Management (SCM) systems or Version Control Systems (VCS) are systems which manage changes to computer programs. They have a set of features that support this activity including version control, rich audit history and multiple streams of change that can co-exist among many others. It is widely accepted best practice that source code should be managed within such a system. This policy specifies the way Digital Services and Technology (DST) utilise Source Code Management.

The policy is based on guidelines set in the GDS Way "How to store source code", when using source control, but there are differences which are identified in this document.

Acceptable Use Policy
1. All source code must be under source control in one of the ONS recognised source control systems (see section in Appendix for this).
2. No sensitive data shall be kept in source control. This includes secrets, keys, private certificates, passwords.
3. Code repositories must be assessed at creation and regularly thereafter to ensure compliance with this policy.
4. Repositories must be created public by default unless you have a specific need for them to be more restricted, this is in line with UK Govt guidelines - Be open and use open source.
5. Code repositories that are not published openly must have the rationale for doing so recorded prominently within the repository using (PIRR).
6. All identities used for access to SCM systems must to be readily attributable to individuals and their organisations.
7. Access to code repositories must be on a least privilege basis.
8. All user authentication to internet facing SCM systems must utilise multifactor authentication.
9. All data exchanged with an SCM system must be protected in transit using encryption.
10. Users with contribute access to the ONS recognised source control systems must have completed mandatory training (see source control specific policy, i.e. GitHub Usage Policy etc).
11. If an application is no longer used in production and there is no update on the repository for the last 01 year, the Technical Lead or nominated Sr. team member should archive the repository, Update the README file accordingly and resolve any open security alerts on the repository.

System specific policy items
- **GitHub:** Please see GitHub Usage Policy.
- **GitLab:** Coming soon.

Principle Enforcement
G6 Program Managers through Technical Leads or Sr. member of respective software development team is responsible for monitoring and enforcing this policy compliance.

Exception process

It is acknowledged that situations arise in which the Policy Detail as above may not be able to be met. Where this is the case a documented policy exception must be sought from the Policy Owner (specified in the table on the title page).

Source Control Advisory Board Members

1. Head of Cloud Services and Support or authorised delegated person;
2. Head of Software Engineering Practices or authorised delegated person;
3. A representative from Security and Information Management (SaIM)

Supporting documents

- Atlassian – What is version control
- GOV.UK Service Manual – Maintaining version control in coding
- GDS – How to store source code
- NCSC – Secure development and deployment guidance
- Central Digital & Data Office – Security considerations when coding in the open

Appendix

ONS Recognised Source Control Systems

GitHub.com Organisations:

- Please see GitHub Usage Policy for the list.

GitLab Instances

- GitLab - General (on premises; available from your laptop/workstation)
- GitLab - DAP (on premises and only available from a DAP virtual desktop)

Note: If you believe there is a recognised source control system not listed above, please contact policy owner.