Integrated Data Service (IDS)
on GCP
Security Operating Procedures

Acceptance			
Version	Name	Position	Date of Acceptance
3.3	Deborah Day	IDS Deputy Director Service and Operations	15/05/2023
3.4	Soph Edgar-Andrews	IDS Deputy Director Service and Operations	16/08/2023
3.5	Soph Edgar-Andrews	IDS Deputy Director Service and Operations	15/12/2023
4.0	Soph Edgar-Andrews	IDS Deputy Director Service and Operations	31/01/2024
4.1	Soph Edgar-Andrews	IDS Deputy Director Service and Operations	01/08/2024

Document Review and Changes			
Version	Author	Owner	Date of Sign-off
1.0	Johanna Salvage	Security Compliance and Audit	21/02/2022
2.0	Johanna Salvage	Security Compliance and Audit	05/04/2022
2.1	Johanna Salvage	Security Compliance and Audit	06/06/2022
2.2	Johanna Salvage	Security Compliance and Audit	12/07/2022
3.0	Johanna Salvage	Security Compliance and Audit	06/12/2022
3.1	Johanna Salvage	Security Compliance and Audit	08/02/2022
3.2	Johanna Salvage	Security Compliance and Audit	06/04/2023
3.3	Johanna Salvage	Security Compliance and Audit	15/05/2023
3.4	Johanna Salvage	Security Compliance and Audit	16/08/2023
3.5	Johanna Salvage	Security Compliance and Audit	15/12/2023
4.0	Johanna Salvage	Security Compliance and Audit	31/01/2024
4.1	Johanna Salvage	Security Compliance and Audit	01/08/2024

Contents

Glossary of Terms

AOC	Assured Organisational Connectivity
API	Application Programming Interface
BYOD	Bring your own device
DSA	Data Sharing Agreement
GCP	Google Cloud Platform
GHES	GitHub Enterprise Server
IDS	Integrated Data Service (available across government and to external researchers)
MFA	Multi-factor Authentication
MoU	Memorandum of Understanding
NCSC	National Cyber Security Centre
ONS	Office for National Statistics
SDC	Statistical Disclosure Control
SyOPs	Security Operating Procedures (specifying the procedural controls for maintaining the security of IDS)
WIP	Work in Progress

1 General Terms

1.1 Applicability and Purpose

The Integrated Data Service (IDS) is a cross-government initiative whereby the Office for National Statistics (ONS) is leading in the delivery of IDS collaboration with partners across government.

These Security Operating Procedures (SyOPs) are only applicable to the IDS and apply to all roles.

The document is designed to articulate the user's accountabilities and responsibilities relating to the IDS; explains what is seen as inappropriate use and sanctions to be applied at both institutional and individual level should misuse occur; and gathers the acceptance of the user to abide by the terms of use laid out. Users of the environment are bound by the laws applicable to data access and the use of information systems, these include the following.

1.1.1 Section 39 of the Statistics and Registration Service Act 2007 (SRSA) and Section 66 of the Digital Economy Act 2017 (DEA):

Make it a criminal offence for any person who has access to personal information held by ONS or a by a public authority to disclose that data to others, subject to a penalty of imprisonment and/or a fine at a level to be determined by the court. Anyone who is discovered to have breached the confidentiality of personal information will be reported for consideration of prosecution.

1.2 IDS User Roles

There are different user roles in IDS to suit different functions, including business use, system management, technical administration, developer, and support. The roles are segregated and associated with different security levels which depend on the data sensitivity and requirement for access to complete the specific function. A list of IDS roles and responsibilities is available in Appendix A.

2 IDS Access and Terms of Use

2.1 Initial System Access

The IDS is designed for business use and it is essential to protect the confidentiality, integrity, and availability of its information. Access to IDS is subject to authorisation and approval. In addition, data access is subject to researcher accreditation and Project approval.

The following conditions must be met by all users:

- Users must take all possible precautions to ensure their screen cannot be overlooked by others;
- Access from public places such as a coffee shop or on public transport is not permitted;
- Users must have updated software and appropriate malware protection (such as antivirus and firewall software) from a trusted provider on their device;
- Users must always lock-screen (with appropriate password protection) their device when they move away from it;

IDS users must not:

- Share or autosave their passwords, pass phrases, PAT token IDs, API keys, certificates etc. or any other information that could be used to compromise access;
- Subvert, explore or knowingly exploit the security features of IDS or the information it contains;
- Introduce malicious software to IDS via deliberate or careless actions;
- Use accounts belonging to other users;
- Share Google IAM accounts and/or password details.

2.1.1 User Account and Password Management

User access to IDS is controlled via login to individual Google IAM accounts where multi-factor authentication (MFA) is enabled. Access to IDS will not be given until MFA is enabled. Users are given a 24-hour grace period, from point of issue, to enable MFA and accounts not registered within this time frame will be locked.

Users must create strong unique passwords. Passwords **should**:

- Be 8 characters for user accounts, and 16 characters for administrators or privileged accounts;
- Be used on every device (e.g. laptop, virtual machine, IronKey) where a user requires an account, protected by multi-factor authentication;
- Be different on every device;
- Contain at least lowercase, uppercase, numerical digit and special characters.

Passwords **should not**:

- Be easily guessable (e.g. date of birth, children, or pet's names);
- Be a word from the dictionary;
- Substitute letters for numbers or special characters (e.g. $1mplet0break!);
- Be re-used or in current use for any other software, hardware, or application;
- Be written down.

Your password must not contain any of the following characters: % ( ) £ .@(Dot followed by @).
Users must not keep a record of individual passwords unless using a secure password manager tool. Passwords and user accounts, as well as Artifactory API keys, must not be shared with anyone. Users must be careful not to share their Artifactory API key with anyone, for example by copying a file that contains the key into a (Work in Progress) WIP bucket. Passwords are used in verification of electronic authentication and to identify users on system audit trails.

The MFA system prompts users for a second form of verification during the login process to prove that access to the application is legitimate as set out in the ONS Password Policy. This ensures that, if a user's password is compromised, an attacker will still be unable to access the account.

To prevent further unauthorised access, users must screen lock their device when not in use or away from the desk. Users must take all precautions to ensure their screen cannot be overlooked by others and must not manually share, photograph, or copy information from IDS.

Any non-compliance will be deemed as a breach of these SyOPs and could contavene conditions as set out in section 6.

2.2 Data System Access

The IDS Data System is defined here as the platform hosting project data: where different controls refer to the Initial System Access this will be explicitly stated.

Before access to the IDS Data System is granted and in order to protect data from unauthorised access, modification or removal, all users must be validated by the Customer Support Team. All users, regardless of their role, must:

- Have the required researcher accreditation and/or security vetting appropriate to their role in IDS;
- Have their access requests set up by the Customer Support Team, with appropriate approvals in place (eg via Lead Analyst or other accountable individual);
- Read, understand, and agree to comply with these SyOPs and all policies listed in Appendix B;
- Sign SyOPs;
- Undertake all relevant security training to demonstrate competence in securely accessing IDS.

In addition, all analyst users must:

- Be a member of an approved Assured Organisational Connectivity (AOC) organisation and have obtained the appropriate organisational signature as detailed in their AOC compliance document to confirm they are the responsibility of said organisation and meet the criteria laid out in the AOC compliance certification framework; or be a fully employed member of ONS;
- Supply the corporate computer name they will use to access the environment.

3 Safe working in IDS Data System

3.1 User Access

Access to IDS is subject to authorisation and approval. In addition, data access is subject to researcher accreditation, AOC agreement, and project approval. All users must abide by any data-specific conditions.

The following conditions must also be met by users:

- Access to IDS data and the IDS Data System is only permitted within the UK;
- Users must only use approved devices relevant to their government department or organisation;
- Users must only work from the locations (home working or remote working and office working) approved for access in their organisations AOC agreement;
- Users must comply with their organisation 'Clear Desk Policy'. Users should highlight physical security concerns to their organisation's security team for escalation to the ONS Security Team.

3.2 Sharing information in IDS Data System with others

3.2.1 Sharing within a Project

Projects within the IDS environment are designed to allow authorised users to share code and results within their project team only. This allows the project team to collaborate, peer review and QA each other's work. Screen sharing is permitted in the following circumstances:

- For collaboration between users within the same project;
- For disclosure control roles to complete output checking;
- For technical support to assist users or authorised individuals with technical queries.

Access and viewing of data held in IDS is only permitted for accredited researchers via an accredited project. Screen sharing for any other purpose is not permitted in IDS. If screen sharing is required (e.g. as part of a demo, etc.), this will be impact-assessed and approved on a case-by-case basis via an IDS Customer Support request to ids.customer.support@ons.gov.uk.

Sharing data in IDS with non-authorised individuals is a breach of these SyOPs.

3.2.2 Sharing Code

3.2.2.1 GitHub

Code must be managed via the GitHub Enterprise Server (GHES) which is a private instance of GitHub only accessible from IDS. The following general principles apply to the use of GitHub (and Artifactory when using it to ingest code):

- No data can be embedded or included with the code;
- Secrets, passwords, pass phrases, PAT token IDs, API keys, certificates etc. or any other information that could be used to compromise access to this or any other system must not be included in the code;
- Users may not move GHES repositories outside the IDS;
- A user guide repository has been created in GHES containing guidance and useful code. Code may be copied from this repository and re-used. In all other cases copying files and code between IDS project repositories within IDS GHES is prohibited;
- The Lead Analyst is responsible for managing and adding users to their project repositories;
- All users must follow the guidelines set out by the organisation in setting up and using GitHub account and repositories;
- An account will be generated for IDS users when they first login, and this account cannot be linked with other GitHub accounts outside IDS.

Non-compliance with the approved processes relating to code sharing will be considered a breach of these SyOPs and appropriate actions will be taken to mitigate any potential risks (see section 6).

Project users are able to request code to be ingested into the IDS GHES from Github.com but all code must be approved by the Lead Analyst. The Lead Analyst may approve code ingest but are not permitted to request code ingests to ensure separation of roles. The Lead Analyst is responsible for reviewing and approving the code ingest and overwrite requests in accordance with the IDS GitHub Repository Importer user guidance and keeping their team informed about any changes. Lead Analysts are accountable for ensuring that all code ingested into their project does not contain data, is legal, within the scope of the project, and does not pose a threat to the IDS environment.

If users wish to make their code reusable by other organisations, or for further guidance in relation to GitHub functionality, contact the IDS Customer Support Team. If data are inadvertently brought into the IDS environment, users must notify the IDS Customer Support Team immediately. Any code needed to be shared with other organisations outside of IDS will only be allowed once the code has been approved and checked through Statistical Disclosure Control.

3.2.2.2 Artifactory

In IDS, download of code libraries and packages via JFrog Artifactory is permissible from repositories and open-source package management systems including PyPi (Python), CRAN, Conda and Debian. Further information and training on the appropriate use of JFrog Artifactory, including guidance on code ingest, is available via the IDS Customer Support Team.

3.2.3 Output Checking

Safe research outputs and code produced in the IDS can be made available to researchers outside of the IDS using the IDS' output checking service. Requested outputs will be checked by IDS staff for disclosure and project governance adherence before being made available to researchers outside of the environment. Statistical disclosure control (SDC) must be applied to all outputs prior to using the output checking service. Guidance on how to prepare outputs and apply SDC will be provided by IDS Customer Support Team.

User activity within the environment is monitored and audited via logs for the purposes of data security and policy enforcement.

Non-compliance with the approved processes relating to this system will be considered a breach of these SyOPs and appropriate actions will be taken to mitigate any potential risks.

4 Data System User Responsibilities

IDS users **must**:

- Have the required researcher accreditation or security vetting, AOC agreement, and approval appropriate to their role in IDS see Appendix A;
- Read and adhere to the policies listed in Appendix B, which apply to all roles in IDS;
- Have their access requests set up by the Customer Support Team, with appropriate approvals in place (eg via Lead Analyst or other accountable individual);
- Abide by and be compliant with any data-specific restrictions and conditions for access, as outlined in supplier DSAs or MoUs (or equivalent);
- Read, understand, and confirm acceptance of this document by emailing 'Declaration of Understanding' to IDS Customer Support and retain a copy for reference;
- Complete all appropriate and necessary system and user training;
- Consider and ensure ethical use of data;
- Inform the Customer Support Team when access changes are required, or access is no longer needed (including maternity leave or long-term sick leave) by emailing IDS Customer Support;
- Have their outputs approved and confirmed via the assured dissemination channel and SDC applied/ethical assessment passed prior to release and dissemination;
- Respond to audit requests from the Security Compliance and Audit Team and any other IDS Audit team;
- Inform the IDS Customer Support Team and ONS Security Teams of any suspected incidents, security breaches, and/or vulnerabilities encountered while working in IDS by contacting the IDS Customer Support Team.

IDS Users **must not**:

- Access IDS using any access method other than via Google IAM;
- Access IDS from any device other than their approved device relevant to their government department or organisation;
- Import, install, or use any unauthorised tools, programs or applications into research projects or the platform;
- Transcribe or ingest data into IDS via an unauthorised route;
- Share screens unless for the permitted purposes outlined in section 3.2.1, or otherwise authorised;
- Access data within IDS for any purposes other than those authorised;
- Attempt to exfiltrate data from IDS through copying, photographing, screenshots or other means, this includes cut and paste of data from a Notebook to a user's device;
- Attempt to print from IDS;
- Attempt to re-identify people or businesses in the IDS data;
- Attempt to bring data or information into their project via an unauthorised route;

5 Legal Constraints

Users of the environment are bound by the laws applicable to data access and the use of information systems, these may include, inter alia, the following:

- Digital Economy Act 2017 (DEA)
- Data Protection Act 2018
- UK General Data Protection Regulation (GDPR)
- Census Act 1920
- The Census (England and Wales) Order 2020
- Computer Misuse Act
- Statistics and Registration Service Act 2007 (SRSA)
- Code of Practice for Statistics

It is the user's responsibility to ensure they do not contravene UK law. For further advice and assistance, queries should be directed to the IDS Customer Support Team. The National Archives; http://www.legislation.gov.uk/ provides a search facility to retrieve current and historical copies of legislation.

6 Non-compliance

Any non-compliance will be deemed as a breach of these SyOPs and subject to sanction. In many cases, a breach could amount to a criminal offence with a maximum penalty of two years imprisonment. Decisions to suspend and/or de-activate users and/or organisations is at the discretion of the ONS Security Team.

6.1.1 Consequences of non-compliance

Person consequences:

- Prosecution under the Data Protection Act;
- Criminal proceedings, which may lead to a fine or imprisonment;
- Re-training and further assessment;
- Reduction in IDS privileges;
- Withdrawal of IDS access temporarily or permanently;
- Removal of researcher accreditation.

Organisational consequences:

- Unlimited liabilities;
- Institutional withdrawal of IDS access temporarily or permanently.

7 IDS Analyst and Organisational Approval and Signatory

IDS User Signatory

Name and address of the user's agreed physical access location (organisation and/or home address):

User Department/Area:

User Computer Name:

By accepting this document, you confirm that you:

- Have read, understood and agree to abide by the conditions set out within the IDS Security Operating Procedures and the policies listed in Appendix B;
- Understand your obligations in relation to IDS access and terms of use and are bound by the laws as stated in Section 5;
- Understand that failure to comply with the terms and intent of the IDS Security Operating Procedures is as outlined within this document, will be treated as a potential breach and will be dealt with in accordance with this document.

User signature: ..... **Email address:** .....

Name (Please Print)	Position or Title	Date

Assured Organisational Signatory (non-ONS users only)

Name of Organisation or institution:

I, as organisational signatory and single point of contact, confirm that the user is the responsibility of this organisation and understand that said organisation could be liable in the event of a breach of this document by the user.

Organisational Signature: ..... **Email address:** .....

Name (Please Print)	Position or Title	Date

ONS IDS Approval

I approve for this user to have access to the IDS platform in accordance with their approved role.

Signature: ..... **Date:** .....

(IDS Customer Support Manager, Office for National Statistics.)

NOTE: Before gaining access to the IDS Data System, users accessing data are required to read, understand and confirm their acceptance to this SyOPs.

Non-compliance with the SyOPs shall constitute misuse of the IDS system. Misuse of the platform or data held in it may lead to disciplinary action and possibly criminal proceedings.

Appendix A – IDS Business and Support Roles

There are several business and support roles in IDS. The roles are associated with different security requirements depending on the level of data and system access required to perform the role. Users in all roles must comply with the policies listed in Appendix B.

IDS Hub Access Roles

Initial System Access allows access to the IDS Hub (this SyOPs relates to the Hub version UI 0.27.0). The IDS Hub enables users to access and search the IDS data catalogue; view useful links such as user guidance, RAS, and Github; and once authorised and approved, access their approved projects in the analytical data system.

Explorer

Role access permissions to be defined.

Data Analyst and Statistical Production Roles

Analyst

Analysts are users of the platform who are given access to data to perform a business role associated with the production of statistics. Analysts must have appropriate researcher accreditation and approval for the data they are accessing. Access is restricted only to data with clear business justification and authorisation.

Lead Analyst

The Lead Analyst is an analyst, within a specific project, responsible for oversight of all work on a project, for monitoring the progress of the project and for providing regular updates on user changes (for example, new project team members joining, users leaving and so on). If the Lead Analyst will no longer oversee a project, because they have a job/role change or similar, they must hand over management of the project to someone else and inform the Customer Support Team.

Deputy Lead Analyst

The Deputy Lead Analyst is an analyst, within a specific project, nominated by the Lead Analyst to fulfil the role of Lead Analyst in the absence of the Lead Analyst. If the Deputy Lead Analyst is no longer able to complete the role, because they have a job/role change or similar, they must inform the Lead Analyst and Customer Support Team so the role can be given to someone else.

IDS Support Roles

All support roles must have SC clearance, a justified reason for access, and the appropriate approvals for access. There are a number of support roles in IDS which cover infrastructure admin and security admin functions, data and project governance audit and compliance, statistical disclosure control, IDS developer, Data Engineering, and different tiers of Customer Support roles.

Managing additional responsibilities

Roles are segregated and associated with different security levels which depend on the data sensitivity and requirement for access to complete the specific function.

There are technical roles concerned with user management and permission and service development. These users can make changes to the environment, but these are logged, and changes controlled and documented.

User activity is monitored, audited and secured with a model of least privilege for the purposes of data security and policy enforcement. Breaches will be taken seriously and may result in written warnings and access to the system revoked as a minimum.

Appendix B – IDS Policies

These policies apply to all IDS users, regardless of the role they have been assigned.

Collecting and Using Special Category Data Policy
Data Ethics Policy
Data Linkage and Matching Policy
Data Protection Policy
Data Standards Policy
Metadata Policy
Research and Data Access Policy
IDS Statistical Research Policy (new release pending)
IDS Output Checking Policy (new release pending)

Appendix C – Change Table

This table details changes that have been made to the SyOPs since the previous iteration. Minor updates, that do not affect users' undertakings, may be added as and when necessary to rectify broken links, typos or to add reference material and will not be included in this table.

Section(s)	Amendment
Document name	Document name amended to read IDS SyOPs and version number.
2.0	Section 2 re-formatted to include sections on Initial System Access and Data System Access. This is to distinguish between users accessing management areas such as the Hub and the platform holding project data. Definitions included.
2.1	The following bullet point 'Access to IDS is only permitted within the UK;' has been amended and moved from section 2.1 to section 3.1. This allows users to access the initial system (i.e., via the Hub) from outside the UK. IDS Data System Access and IDS project data access remains from within the UK only.
3.2.2.1	Additional sentences added to cover users bringing code into IDS and the responsibilities of the Lead Analyst.
3.2.3	Data Dissemination section renamed to read Output Checking. Wording in this section also revised to better reflect current output checking terminology and processes.
Signatory	Removed requirement for users to supply MAC (Media Access Control) address information. This has been removed in line with available security services and on advice from DPO in line with data minimisation principles.
Appendix A	Included additional sentence under IDS Hub Access Roles to summarise the IDS Hub and what it enables users to do.
Appendix A	Removed reference to Standard and Enhanced User (researcher/analyst) roles as there are no existing users under these roles and role has been replaced by the Analyst role which has the same permissions.
Appendix B	IT Acceptable Use Policy and Guidance reviewed and removed as attached documents. Additional and relevant policy and guidance points embed into section 2.1 of the SyOPs.

SyOPs release schedule from January 2025:

1st February	Full release n.0
1st May	Pre-release n.1
1st August	Pre-release n.2
1st November	Pre-release n.3