Department
for International
Development

Security Policy for Contractors / Consultants / Suppliers

1. This document specifies the requirements that must be met by contractors in the handling, management, storage and processing of information belonging to DFID or its partners.

Information Security

2. Information security is the preservation of confidentiality, integrity and availability of DFID information. Information risk means the risks to the security of DFID's information.

Objectives

3. DFID requires the security of its information to be maintained in order to ensure that DFID is able to rely on its information for its business needs and meets its statutory, regulatory and HM Government policy obligations.

4. DFID imaintains an Information Security Management System and applies security controls consistent with ISO 27001:2013 .

Information Risk Assessment and Management

5. DFID employs risk assessment methodologies consistent with HMG guidance (NCSC Risk Management Introduction).

6. Residual information risks can only be accepted by the DFID Senior Information Risk Owner, their Deputy or the DFID Accreditor to agreed levels.

Legislative, Regulatory and Contractual Requirements

7. The management of DFID and other official information may engage obligations under the following legislation (note that this list is not exhaustive):

    - Official Secrets Act 1989
    - Public Records Acts 1958 and 1967
    - Data Protection Act 2018
    - Freedom of Information Act 2000
    - Environmental Information Regulations 2004
    - Human Rights Act 1998
    - Computer Misuse Act 1990
    - Copyright (Computer Programs) Regulations

- Civil Evidence Act 1968
- Police and Criminal Evidence Act 1985
- Wireless Telegraphy Act 1949
- Communications Act 2003
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Civil Contingencies Act 2004

8. DFID is required to comply with HM Government policy on information security and assurance including:

    - The Security Policy Framework
    - The Government Security Classification Policy
    - HMG Information Assurance Standards

9. Any organisation accessing, processing, communicating or managing DFID's information must do so such that DFID's legal, policy and regulatory obligations are met.

10. Where Data Controller DFID must specifically authorise, having consulted the DFID Data Protection Officer, any processing of personal data outside of the UK or European Economic Area (EEA). Such agreement and arrangements for data processing must form part of a contract between DFID and Data Processors.

11. Anyone accessing official information through provision of goods or services to DFID will be bound by the terms of the Official Secrets Act 1989.

Access to DFID Information, Information Assets and Information Systems

12. Anyone required to access DFID information and/or work in a DFID building must either hold or be prepared to apply for a Baseline Personnel Security Standard (BPSS) clearance. This entails identity, nationality and criminal record checks. BPSS clearances obtained through other government departments may be accepted by DFID. If access is required to information at higher levels of security classification, additional national security vetting checks may be required.

13. Access to information assets and systems will be the minimum necessary to achieve business purposes.

14. When the need to access DFID information, assets and systems ends, all DFID equipment (e.g. laptops, security passes, etc) must be returned to DFID prior to the termination of a contract.

15. DFID may monitor the use of its information, information assets and information systems for lawful business purposes.

16. Anyone granted access to DFID information, information assets and systems must comply with the requirements of DFID's Security Manual including its Acceptable Use Policy. Failure to comply with these policies and other relevant instructions may constitute a breach of contract and lead to termination or legal action.

17. Removable media (including laptops) may only be used to manage DFID information with the explicit consent of DFID. Any removable media must be encrypted to a degree commensurate with the security classification of the information held within the removable media as required by HMG standards.

18. Supplier personnel may only enter DFID premises with an appropriate security pass issued by DFID and may only enter areas of DFID premises commensurate with their function and, where appropriate (for example, in security areas), escorted by DFID staff.

Information Security Management System Controls

19. Where a supplier is contracted to manage DFID information, information assets or information systems, the supplier must ensure that an information security management system employed to secure DFID information, information assets or information systems is in place and complies with ISO/IEC 27001. Evidence must be provided to DFID of compliance with the standard, either through formal certification or otherwise to DFID's satisfaction before any DFID information, information assets or information systems are accessed by the supplier.

20. Suppliers must agree to permit and facilitate audits of all aspects of their information security management system by DFID and to address any findings of such audits in order to preserve the security of information to DFID's standards and requirements.

21. The transmission of information between DFID and a supplier must be encrypted to a level commensurate with the security classification of the information and to HMG standards.

22. Live DFID data and information may not be used for test purposes. Data and information to be used for test purposes must be anonymised, scrambled or otherwise rendered in such a way that no live DFID data or information can be reconstructed from that used for test purposes.

23. DFID information may not be copied by any supplier other than as far as is necessary for providing an agreed service to DFID.

24. Suppliers must have a security incident reporting process in place to a standard and design acceptable to DFID to ensure that any incidents involving DFID information are immediately reported to DFID. Suppliers must agree to undertake any remedial action required by DFID and ensure that this is implemented in an auditable way.

25. A supplier holding DFID data on DFID's behalf must have in place processes to ensure that critical DFID information held by them can be promptly and efficiently recovered following an emergency.