# Blue Book

# H – Security

## *H1. Security*

### Background

DFID, in common with other Government Departments, is responsible for assessing its own security risks and setting appropriate policies and procedures to mitigate these in the context of its business objectives and in line with central government rules and guidance.

All UK based staff are bound by the provisions of the Official Secrets Act governing the disclosure of information.

All staff are bound by the departmental security rules and procedures. Staff should ensure they are familiar with and apply these rules. Line Managers are responsible for ensuring compliance in their work areas. Heads of Office/Department are accountable to Directors for ensuring security policies and procedures are adapted to local environments and implemented. Directors, supported by Heads of Office, are accountable for ensuring that duty of care is fulfilled for all staff working in their Division.

The Departmental Security Officer (DSO) and Departmental Security Unit have overall responsibility for promulgating security policy, guidance dissemination and monitoring compliance. The Security Committee reviews and assesses security policies.

DFID security procedures are informed by the rules and guidance contained in the Cabinet Office Security Policy Framework (replacing the Manual of Protective Security). DFID's Security Manual and other guidance on the Security web-page on Insight summarises key security rules, processes and responsibilities. Heads of Office, Cabinets and Overseas Security Managers also have access to detailed overseas security guidance on the Security Managers Team site.

Unless otherwise specified all security compliance matters apply equally to all DFID offices, whether in the UK or overseas, and are equally as relevant to UK based and Staff Appointed In Country (SAIC) staff, as well as temporary, casual or consultancy staff working in our offices.

Failure to comply with security policies and procedures may be recorded as a security breach and may be subject to disciplinary action taken. Unauthorised disclosure of official information may be regarded as a leak and be subject to disciplinary action.

## Compliance Tasks

1. Staff must wear building access photo passes visibly at all times while on DFID premises. However passes should not be worn outside of the office. The loss of a pass should be immediately reported to Departmental Security Unit. Visitors to the office must be escorted at all times.
   **Task assigned to: All staff**

2. All information (whether in hard copy, on computer systems or on storage media) must be assessed and appropriately classified in line with the government protective marking system by the originator of the information. Information should be communicated, stored and (when necessary) destroyed in accordance with security management procedures related to the classification of the information involved. Detailed guidance is given in the DFID Security Manual at the Security web-page. Access to Restricted and more highly classified material is governed by the "need-to- know" principle.
   **Task assigned to: All staff**

3. Equipment and physical assets must be recorded in the DFID asset register and suitably secured both in and out of the office (eg. laptops when travelling) to safeguard from theft and/or misuse. Advice on storage and handling is given in the DFID Security Manual.
   **Task assigned to: All staff**

4. DFID buildings in the UK and overseas must have physical security measures, procedures and rules in place commensurate with the perceived threat. Security Section directly manages physical security aspects in UK buildings. Each Head of Office is responsible for ensuring that overseas offices maintain appropriate protective security measures, drawing on advice and recommendations from the FCO

Overseas Security Advisers (OSA). OSA recommendations must be implemented fully and promptly unless a Director agrees a waiver.

**Task assigned to: Head of Overseas Office, Overseas Security Managers, Departmental Security Unit**

5. All staff posted overseas (and frequent travellers) must attend or receive an appropriate overseas security awareness briefing before posting/travelling.
   **Task assigned to: All staff**

6. All HCS and SAIC staff posted to or travelling to Fragile Environments must receive security briefings and attend specific security protection courses (i.e. SAFE training) before posting. Briefings will be managed locally by Heads of Office, in consultation with Security Section and local FCO management. SAFE trainig must be undertaken before travel.
   **Task assigned to: All staff, Head of Overseas Office, Overseas Security Managers**

7. All staff posted overseas and visitors must receive a local in-country security briefing at Post on (or before) arrival.
   **Task assigned to: Head of Overseas Office, Overseas Security Managers**

8. All breaches of security procedure, thefts and losses must be reported to Line Management and Departmental Security Unit immediately on detection. Thefts and losses of IT assets must be reported to Departmental Security Unit via a Security Incident Report.
   **Task assigned to: All staff ,Departmental Security Co-ordinator, Line Manager**

9. All DFID staff (including SAIC) and other personnel working in a DFID office or accessing a DFID e-mail account (consultants, contractors, temps etc.) must as a minimum be cleared to the Baseline Personnel Security Standard (BPSS). Baseline Standard checks will also apply to staff DFID is recruiting on behalf of others.
   **Task assigned to: All staff**

10. National Security Vetting (CTC, SC or DV level) is required where staff and other personnel working for DFID require access to higher level classified information. Departments must submit a case to Departmental Security Unit setting out the rationale for higher level clearance. The level of security clearance is specific to the post rather than individual and must be related to the actual requirements of the job. Departmental Security Unit oversees and manages clearance procedures in line with Cabinet Office guidance. Further advice is contained in the DFID Security Manual and in the "Handy Guide to Security Clearance".
    **Task assigned to: All staff**

11. Every department in the UK must have a Departmental Security Co-ordinator (DSC). They and their deputies are responsible for coordinating security within their departments and providing a first line response on some security issues eg. re-setting combination locks. Departmental Security Unit provide overall advice and co-ordination of DSCs.
    **Task assigned to: Head of Department**

12. Every DFID overseas office must have a Security Manager who will report to the Head of Office on all security issues. The nature of this post will vary from office to office and may be a part or full-time job.
    **Task assigned to: Head of Overseas Office**

13. Overseas Offices must report Security Incidents, including near misses, to Security Section using the Security Incident Report form.
    **Task assigned to: Head of Overseas Office, Overseas Security Managers**

14. Directors will produce an annual security assurance statement for each of their Divisions.
    **Task assigned to: Director**

### Risks of non-compliance

- Vulnerability of DFID buildings and staff to terrorism, espionage and theft
- Inappropriate disclosure of information
- Loss of Information or breach of confidence
- Loss of equipment
- Prosecution and official criticism
- Damage to reputation and impact on DFID credibility within Whitehall and overseas
- Failure in duty of care to staff and others
- Actual harm to personal privacy, commercial confidentiality, international relations, candour of internal discussions, willingness of partners to share information etc
- Legal challenge to DFID for acting incompatibly with the 1998 Human Rights Act (HRA).

## *H2: Security – information risk management*

### Background

DFID defines Information Risk as that part of DFID's overall risk portfolio which relates to the Confidentiality, Integrity and Availability of information within the organisation, in electronic and paper forms. It is vital that we manage these risks well in order to minimise the potential impact on DFID's operations and reputation, and to protect any personal information which we look after on behalf of the public.

This is relevant whether data is in storage, processing, or transit and whether threatened by malice or accident.

The Management Board owns DFID's overall processes for managing risk. Information risk is managed in the same overall framework as other risks in DFID, but with specific ownership, accreditation and monitoring arrangements in place which employ best practice principles drawn from external and HMG standards.

DFID's policy for managing information risk and evaluating the effectiveness of the measures put in place is the responsibility of the Finance & Corporate Director-General who takes the role of Senior Information Risk Owner (SIRO). There is also a Deputy SIRO, the Head Of Business Solutions Department who can satnd in for the SIRO when required.

The SIRO is responsible for developing and implementing this policy and for reviewing it regularly to ensure that it remains appropriate to the business objectives and risk environment.

The SIRO also appoints an Information Security Management Group (ISMG) to advise on the overall management of information security and information risk. This is chaired by the Deputy SIRO.

DFID has adopted the International Standard ISO27001 to manage this process and as a mechanism for managing our information related risks. As part of this process, DFID is subject to periodic audit and inspection by external auditors who will assess compliance with the International Standard and identify non-conformities.

DFID holds a relatively small amount of personal data and a moderate amount of information which is classified at Restricted or above. On occasions, some of this data is shared with delivery partners, including commercial companies and other Government departments. Management

and sharing of information must comply with the Data Protection Act and other legislation.

Threats to DFID's information come from a variety of sources inside and outside the organisation. These are assessed on a continuing basis by the IT Security Officer, taking advice from HMG sources as required.

The standard DFID "whistle-blowing" procedure may be used to report suspected breaches of information security.

Any data loss incidents must be reported in the DFID's Annual Report and in the notes to the Annual Accounts.

Staff are reminded that misconduct which leads to the compromise of DFID information will be taken seriously and can lead to disciplinary processes.

## Compliance Tasks

1. All Information Assets (electronic and paper) in DFID must be catalogued by Business Systems Division and an Information Asset Owner appointed within the relevant part of the DFID business.
   **Task assigned to: All staff, Head of Department, Head of Overseas Office, Information Asset Owner**

2. All systems and processes which share personal, sensitive data with delivery partners must be approved in advance with the relevant Information Asset Owner.
   **Task assigned to: All staff, Head of Department, Head of Overseas Office, Information Asset Owner**

3. The Information Asset Owner is accountable for ensuring that the risks of data sharing are assessed and appropriate mitigation steps taken. Advice must be sought from the Openness Unit, Knowledge

Information and Management Team, on compliance with the Data Protection Act and other legislation.

**Task assigned to: All staff, Head of Department, Head of Overseas Office, Information Asset Owner**

**4.** The Information Asset Owner must formally log all data transfers with delivery partners.
**Task assigned to: All staff, Head of Department, Head of Overseas Office, Information Asset Owner**

**5.** Each Information Asset Owner must review their assets at least annually in line with HMG guidance and provide a summary to the SIRO.
**Task assigned to: All staff, Head of Department, Head of Overseas Office, Information Asset Owner**

6. The IT Security Officer must maintain a log of information security incidents and report on recent incidents to each meeting of the ISMG.
**Task assigned to: All staff, Head of Department, Head of Overseas Office**

**7.** All methods used to hold or carry material classified at Restricted or higher must be documented with a Risk Management Accreditation Document Set. This classification of risk must be carried out by someone with experience and suitable qualifications in risk assessment, such as a Departmental Accreditor or a CLAS consultant.
**Task assigned to: All staff, Head of Department, Head of Overseas Offices**

8. IS standards include methodology to assess risk levels. DFID must not accept risks which are assessed as Medium-High or above. Risks which are assessed as Medium must be referred to the SIRO for acceptance. Risks which fall below Medium are assessed and certified by the Department's IS Standards accreditor. Current risk levels are: Low, Low-Medium, Medium, Medium-High and High.
   **Task assigned to: All staff, Head of Department, Head of Overseas Office**

9. All new IT systems, and all substantial upgrades to existing IT systems, are subject to a risk assessment in according to HMG Information Security standards before they are implemented.
   **Task assigned to: All staff, Head of Department, Head of Overseas Office.**

10. All new IT systems which hold personal data must be subject to a Privacy Impact Assessment (best practice) before implementation.
    **Task assigned to: All staff, Head of Department, Head of Overseas Office**

11. If, following completion of a Privacy Impact Assessment, a full Risk Assessment is required, DFID's Security Officer must be consulted for advice and for access to certain documents and guidance that are classified and therefore only available through the Government Secure Intranet (GSI). These include:

    a. Risk Assessment - Infosec1, Part 1 & 2
    b. Risk Management - Infosec 2
    c. Connecting Business Domains - Infosec 3
    d. Cryptography - Infosec 4, Parts 1, 2 & 3
    e. Secure Sanitation - Infosec 5

f. Advisories - EIP Security Notices

g. Guidance - CESG Infosec Memoranda

h. Standards - CESG Infosec Manuals

i. Best Practice - CESG Good Practice Guides

j. Security - CESG Security Procedures

k. Security Responsibilities - Manual of Protective Security.

**Task assigned to: All staff, Head of Department, Head of Overseas Office**

**Protecting Information**

12. All new staff or those transferred into posts where the handling of Personal Data is part of the job must complete the Responsible for Information General User E-Learning module. It is the responsibility of the line manager to ensure that this takes place.
**Task assigned to: All staff, Head of Overseas Office, Line Manager**

### Risks of non-compliance

- Potential security breaches or data loss
- Damage to DFID's reputation
- Disciplinary processes will be applied to misconduct which leads to compromised information
- Legal action resulting from data loss causing harm or embarassment to an individual.

## *H3. DFID Travel Clearance Approval Policy*

### Background

DFID policy is that all staff travel decisions to areas where FCO advise against all travel must be taken by Regional Directors. In departments where there is no Regional Director decisions are delegated to the departmental

head, who will copy the DG in the final decision correspondence. For cross-government coordination and awareness purposes, completed MENAD TCAs must still be sent for information to TCA email box in advance of the trip.

DFID Regional Directors are required to approve DFID staff travel to areas for which an FCO travel advisory warning is in place that advises against all travel. The FCO Travel Clearance Approval (TCA) form must be used for all such requests.

FCO must be consulted and informed of such requests and invited to provide advice or comment. The final decision will rest with the relevant DFID Regional Director. The flowchart at Processes and Tools sets out the required authoristation process.

Please note: Duty of Care responsibility resides with the employer. Permission to travel for non-DFID staff, including contractors, should be sought from the relevant department or employer. Where travelling parties include staff from other Government Departments their respective risk holders must be made aware and consent to their staff participation. FCO will have a coordinating role in such cases.

Permission to undertake non-duty travel to regions where the FCO advises against all travel should also be sought from the relevant DFID Director.

**Compliance tasks**

1. TCA form raised by DFID Office/team.
   Full details of the proposed trip including a business case, participants, itinerary, risk assessment, and plans for transportation, accommodation, medical treatment and communications must be included.
   **Task assigned to: All staff**

2. FCO consulted locally.
   The Overseas Security Manager at post, or regionally covering the

post, must be consulted. The OSM comments are made in a box at the end of the form marked `OSM'. The post security officer (PSO) must also be consulted, and any comments from the PSO recorded in the box at the end of the form marked 'Post'.

**Task assigned to: Overseas Security Managers**

3. Submit TCA.

   Forms must be submitted to the TCA email box routinely not less than four (4) working days before travel is to take place. The email subject line must start with 'TCA ROUTINE'. Four working days is the minimum time to inform and consult with FCO Regional desk officers and ESD before submission to DFID Regional Directors, and still allow Directors adequate time to consider an application. Where less than four working days but more than 24 hours is available, TCAs are to be submitted with the email subject line starting 'TCA URGENT'. In emergencies where 24 hours or less is available a TCA must be submitted with the subject heading 'TCA EMERGENCY' and the DFID Regional Director notified directly by the submitting team/office.

   **Task assigned to: Director, Overseas Security Managers**

4. DFID DSU forward TCA forms to FCO ESD Desk officer on the same working day of receipt. FCO ESD will consult and inform internally including relevant FCO Regional Directors. Any comments will be returned to the TCA email box within two working days. FCO ESD has a coordinating function across HMG, but is also an important source of advice to DFID Regional Directors in taking decisions on TCAs, and part of the support they should draw on in discharging this responsibility. FCO ESD is formally engaged to provide advice under a Service Level Agreement with DFID.

   **Task assigned to: Director, Security Section**

5. DFID DSU forwards completed TCA to DFID Director
   The TCA now bearing comments from FCO OSM/PSO at post, and potentially comments from FCO ESD/Regional Desk is submitted to DFID Regional Directors with any additional security observations or comments from DSU to DFID Regional Director with recommendation to approve or reject. DSU has a role in quality assuring TCAs against OSA recommendations, current intelligence reporting, and DFID Security Committee policies.
   **Task assigned to: Director, Security Section**

6. DFID Regional Director within two working days approves or rejects TCA, and directly notifies DFID office/team raising TCA.
   **Task assigned to: Director, Security Section**

7. Directors are responsible for retaining records of travel clearance authorisations within their regions.
   **Task assigned to: Director**