

Blue Book

I – Information systems

I1: Information systems

Background

DFID's IT network links the main HQ offices in the UK to over 70 other DFID offices around the world. It allows for the transfer of data between these offices and access to centrally held systems.

The use of home working facilities and remote laptops throughout DFID helps to support the DFID's "Finding a Fit" and "Work Life Balance" initiatives.

DFID has a limited number of terminals that allow access to FIRECREST-D and these have been deployed at most sites. This has led to increased security requirements. FIRECREST- D is the DFID version of the FCO CONFIDENTIAL FIRECREST system.

DFID's disposal policy is to donate Personal Computers (PCs) to charities and aid projects and we insist that the hard disk is securely wiped and that this is verified. This ensures that all DFID data is removed, including licensed software, which we cannot transfer to a new owner.

Staff will have to comply, when disposing of IT Equipment, with the Waste of Electrical and Electronic Equipment (WEEE) guidelines that will become law during 2007. The recipient of any equipment from DFID will also have to confirm it will be disposed of in accordance with the WEEE regulations.

Misuse of IT systems will result in disciplinary procedures against staff.

Compliance Tasks

1. DFID's Network and DFID Laptops are classified as RESTRICTED. Users' files must not contain information requiring a higher protective marking
2. Passwords used to access the network must not be disclosed to anyone else. Disclosing or sharing a password will constitute a security breach

Task assigned to: All Staff

3. Users must not install or use software that has not been authorised and approved by ISD. Details of the supported software can be found in the ISD

Service Level Agreement (SLA)

Task assigned to: All Staff

4. Staff must verify that the recipients have the necessary access rights before sending them a RESTRICTED document by e-mail. Restricted E-Mails that are sent to external (non dfid) recipients should be sent via the GSX E-Mail system and not the normal DFID E-Mail system.

Task assigned to: All Staff

5. All equipment loaned from ISD must be signed for by the user

Task assigned to: All Staff

6. Users must ensure that all IT equipment is safely stored and protected both in and out of the office to safeguard it from theft/misuse. Users must lock their computers when they are unattended using password-protected screen-savers. Laptops must also be secured using Kensington Locks when they are unattended. Laptops containing RESTRICTED material must be handled according to the rules for RESTRICTED documents

Task assigned to: All Staff

7. Before staff leave DFID employment, they must return all IT equipment that was given to them. Users must receive training before they can be issued with a remote working laptop

Task assigned to: All Staff

8. The FIRECREST-D system is classified as CONFIDENTIAL. Users' files must not contain information requiring a higher protective marking. From January 2009 the FIRECREST-D system will be connected to the X-GSI. This will allow confidential E-Mail transfer to other Govt Depts that are on the X-GSI network. This system is for confidential E-Mails.

Task assigned to: All Staff

9. All new users MUST be SC cleared (Security Clearance) by the Security Section before being given access to FIRECREST-D machines

Task assigned to: All Staff

10. From January 2009, DFID will have a secure Videoconferencing unit in Palace Street. This will be used for connection to the FCO secure Videoconferencing system and will be for confidential conferences.

Task assigned to: All Staff

Risks of non-compliance

- Potential Security Breaches
- DFID IT Infrastructure put at risk
- Damage to DFID's reputation
- Introduction of Viruses to DFID Network
- Integrity of DFID network put at risk
- Potential for unnecessary downtime.

Associated learning and skills

Users will not be given a remote working system without prior training
Help Desk Facilities - The Help Desk will provide full user support from 02:30 - 19:00 (UK Time) during normal working days. Support from 02:30 to 07:00 UK time is provided by DFID staff based in Delhi.