Skills Development Scotland

Appendix 9

SDS Information Security Policy

Background and Purpose

The purpose of this document is to outline the required behaviour of Providers when using the Skills Development Scotland (SDS) **Funding, Information and Processing System** (CTS/FIPS). The rules are defined to protect the interests of SDS and the organisations contracted to deliver National Training Programmes on behalf of SDS. The intention is not to impose intrusive constraints that are contrary to our established culture of openness, trust and integrity, which SDS recognise as essential contributors to the success of SDS. Information Security is committed to protecting the operation and reputation of SDS in fulfilling its role as the catalyst for real and positive change in Scotland's skills performance. This document applies to all National Training Programme information processed by and on behalf of SDS.

Responsibility

- All organisations contracted to deliver national training programmes are responsible for implementing, enforcing and adhering to the provisions of this policy
- All contract signatories are responsible for ensuring this policy is adhered to
- All company employees are responsible for ensuring visitors are also aware of this policy and are supervised appropriately

Policy

Any Provider in breach of this policy will be in breach of Provider Contract with SDS and may have their contract terminated.

Policy Statements

1. CTS/FIPS can be accessed using your own CTS/FIPS login id. Do not leave clues or evidence of passwords near to your computer.
2. Using another person's login id is not permitted under any circumstances.
3. Passwords must not be saved on any login screen, i.e. do not tick 'Save Password' or 'Remember Me' options if these appear.
4. Never leave a logged-in computer unattended when using CTS/FIPS. Use the Windows (or operating system equivalent) 'Lock Workstation' facility (Windows key + L) or logout.
5. Protect against accidental compromise of SDS information; ensure information cannot be observed by unauthorised people, clear away all material and documents at the end of the day, and do not leave documents in printers or copiers.
6. Deliberate, unauthorised entry to CTS/FIPS, entry of false data and unauthorised changes to information are strictly forbidden.
7. Providers must report all CTS/FIPS security incidents. In the first instance please contact the system helpline (appropriate SDS department) who will ensure the correct handling of the incident.

8. Data extracted or originating from the CTS/FIPS must be encrypted or transferred in a secure manner when forwarding to SDS.
9. SDS may, at its discretion, and without prior notice change the Information Security policy.

Data Encryption

Data Encryption is a requirement of SDS where personal data, including CTS/FIPS data, is being transferred from and to third party organisations including Providers. SDS currently utilise WinZip to encrypt files with 256 bit AES encryption. All data transfers between SDS and third parties must use compatible encryption software (for WinZip version 9.0 and greater is compatible). Each data transfer will be to a named contact by means of an encrypted Zip file that will have a password. On receipt of the file the recipient must contact the originator to obtain the password. The password must not be transmitted by the same means as the encrypted data file. Data transferred back to SDS must also be encrypted.

The encrypted file may be transmitted by email. Where encrypted files cannot be transferred by this method they should be burned to CD and posted using double envelopes or hand delivered. If encrypted files are not available, hard-copy documents must be posted using double envelopes or hand delivered.

It is the responsibility of the Provider to provide their own copy of the necessary encryption software.