



Data Transfer Standards

Publication date: 10 April 2008

This document outlines the Marketing Association's Data Advisory Network's recommended data transfer standards. This document assumes that both the sender and recipient have the relevant security in place for the storage of the information at their premises.

The transfer of data from one location to another happens every day within organisations. Methods range from one-off delivery of data on a CD from one company to another, through to real time delivery of information over the Internet. Given this, the data needs to be adequately protected when it is transferred.

Why are these standards required?

The protection of information about individuals and companies is crucial within business. Consumers and businesses give information on the understanding that their information will be well managed within the organisation that collected it, and that if the information is transferred in any way, and then it will be done in a secure manner.

Recent occurrences of sensitive data going missing (e.g. 25 million UK personal details in late 2007) have shown that some organisations are not following best practice.

Considerations:

There are three core areas that need to be addressed when transferring information. They are:

- Data
- Encryption
- Transfer

Each of these areas is covered in more detail below.

1. Data

It is recommended that only data specifically required by the recipient be included in any data transfer. For example, if customer date of birth is not required, then do not include it in the data extract for transfer.

Each organisation should have a classification system for data, and agreed methods for the protection and transfer of that information. The data classifications may be similar to those below:

A) Strictly Confidential

B) Confidential

C) Sensitive

D) Commercial

Consider the legal, privacy, contractual and commercial restrictions on any data that is to be transferred.

2. Encryption

For information that is being sent externally, and according to the above classifications would be considered sensitive, confidential or strictly confidential, the Marketing Association's Data Advisory Network recommends that the information be encrypted with 128 bit technology or better. It is worthwhile considering the implications if the information does get into undesirable hands.

Note: The Privacy Commissioner is developing guidelines in the event that data is leaked, including communication to customers.

2.1 Single-key encryption

Single key encryption is where both the sender and recipient have the same password, that is, the sender encodes the file with the same password that the recipient uses to open it. Compression products such as WinZip 9.0 upward offer this type of encryption to an acceptable security level (128 bit encryption technology or better).

Note: Previous versions (before 9.0) of WinZip use weak encryption that is easy to decipher. A password by itself will deter people, but strong encryption and a good password are required to ensure that the files are secure.

It is not recommended that confidential information be encrypted with single-key encryption as the password can be shared among multiple people, within multiple organisations.

2.2 Public/private encryption

The recipient of the information nominates two types of key, or password.

The first key is a public key, which is given to the sender of the information to enable encryption of the information. However, this key cannot be used to decrypt the information.

The recipient has a private key or password that is only known to them. This key enables them to decrypt the information.

There are two main advantages of public/private key encryptions over single key encryption:

1. The recipient may share the public key with multiple people, as they are only able to encrypt data with the key
2. The decryption stays within the one organisation, hence lowering the chances of unauthorised people being able to decrypt the data

Programmes such as PGP® are available for public/private encryption of files. For file transfer, it is also possible to set up firewalls to enable file encryption when transferring between predetermined locations or IP addresses.

Again, the Marketing Association recommends 128 bit encryption as a minimum for public/private encryption.

2.3 Password protection

Ensure that encrypted files are password protected. It is recommended that the password be at least eight characters long. You should keep the following considerations in mind when choosing passwords for your files:

- In general, longer passwords are more secure than shorter passwords. In fact, taking maximum advantage of the full strength of encryption requires a password of approximately 32 characters for 128-bit encryption and 64 characters for 256-bit encryption.
- Passwords that contain a mixture of letters (upper and lower case), digits, and punctuation are more secure than passwords containing only letters.
- Because you can use spaces and punctuation, you can create "pass phrases" that are long enough but still easy to remember and type.
- Avoid using easily guessed passwords such as names, birthdays, IRD numbers, addresses, telephone numbers, etc.

When giving single key passwords out to other parties, ensure that you use a different form of communication than that by which the data is sent. For example if you are emailing the encrypted document, then communicate the password via a phone call.

Never give private passwords to people external to your organisation.

3. Transfer

3.1 Physical

Ensure that the media (CD, DVD, tape, disk etc) is well packaged and labelled. Make sure you are able to find or trace the package eg:

- Courier – ensure that a signature is required as well as track and trace
- Post – ensure that a track and trace is available on the item
- In person – ensure that the person who is delivering the data is aware of its confidential status

Once received and verified, the media should either be destroyed or stored in a secure area. Each organisation should have a policy around the storage and destruction of information.

The prevalence of memory sticks to transfer data is growing. If memory sticks are used, then it is important that the data is erased from the memory stick and if confidential information is involved that the memory stick is overwritten to ensure the destruction of the data on the stick.

3.2 Internet

The transfer of information via the internet is very common. Two main forms of transmission exist:

- A file transfer protocol
- Email

On receipt of the information, the recipient should check its validity, confirm receipt with the sender and then delete the data from their mail system or file system. Likewise, the sender of the information should delete the information from their mail system or file system once the data has been received and verified by the recipient.

Even if a secure link (eg dark fibre or direct frame relay) network is used, it is still recommended that data be encrypted.

Firewalls: if sending/receiving encrypted files by email you may find that your firewall or email server blocks the file as it cannot "inspect" the contents of the file. In these situations will need to liaise with your IT team to have the file "released" to you.

To download a copy of these standards, go to www.marketing.org.nz/best_practice.php

Review Period, 1 year from publication date.