DMA Information Security Management Requirements January 2015

DMA Standard: produced for the protection of electronic information.

INTRODUCTION

Information within an organisation can take many paths and can be used for many varied purposes. This data flow is unique because every organisation has different processes and uses information in different ways. Some of the information can be mundane, other information can be personal or sensitive.

It is therefore important for organisations to ensure that their data security practices deliver appropriate protection for these various data journeys – not only within their organisation but also with third party suppliers.

This is especially important for information used for marketing purposes. Whether it's the transmission and storage of electronic information or its effective safeguarding through systems, physical security or access control it's essential that security measures are applied which demonstrate a total understanding of the potential risks that each of these journeys represent.

When an organisation takes time to understand this flow and the sensitivity of the data, security can be greatly improved by applying a strategic, proportionate and professional approach to information handling.

DATASEAL OVERVIEW

This document identifies the security requirements that each participating organisation must implement, as appropriate, in respect of the data that is captured, used, stored and transferred by the organisation.

The document recognises that the use and storage of data on computers and files and the transfer to third parties is a required part of legitimate business. Commensurate with that requirement is the need for appropriate security measures to protect the confidentiality, availability and integrity of such information. These requirements recognise that not all companies are the same and that data is used differently by various processes and arrangements.

As a consequence, each organisation must clearly define the scope of their proposed DataSeal certification describing physical locations and, where necessary, departments, functions and any dependencies or third parties. This is particularly important for larger organisations that may also need to identify scope boundaries and areas that are out of scope.

At its launch in 2010, the DataSeal standard was initially developed to help improve the information security practices of DMA 'supplier' members that under the Data Protection Act are defined as 'data processors', i.e. any organisation who processes personal data on behalf of a client, or 'data controller'. By contrast a data controller is defined as the organisation that determines how and why data is processed.

However, during 2011 the standard was made available to members of other marketing trade associations and has now become the UK standard for information security in the marketing industry.

As a consequence, the DataSeal standard has been further refined and developed to reflect the specific information security challenges of both data controllers and data processors.

The assessment criteria have been based on the expected use of technology and information by members of DMA and other participating trade associations. Should any organisation have technology capability that makes complying with these requirements impossible, the details of non-compliance must be reported to the DMA via compliance@dma.co.uk and will be reviewed and approved on an individual basis. Notification of such 'non-compliance' must include details of the alternative steps that the organisation will take to provide an acceptable level of security.

A higher level of Information Security can be demonstrated by obtaining certification to the International Standard on Information Security ISO 27001.

Compliance to these requirements will be independently verified on an annual basis. In most cases this will likely require a one day assessment although larger or multi-site organisations may require additional audit days.

If an information security incident, loss of control or complaint about a DataSeal certified member is received, the DMA in its capacity as scheme administrator may instigate a further investigation / inspection which could take the form of a partial or full re-audit of the member. Any and all breaches in information security affecting data will be reported by the DataSeal member to

the DMA within 48 hours of discovery. Depending upon the nature of the breach, the DMA may request that the member notifies the relevant enforcement bodies, including the Information Commissioner's Office (ICO).

The DMA also reserves the right to suspend and/or completely withdraw DataSeal certification in the event of such a breach, following subsequent investigation.

Throughout the document the terms must and should are used carefully and deliberately. "must" is not negotiable; the term "should" is used where a requirement is considered best practice and are goals for the organisation. The terms data and information are used and are interchangeable. The terms system and network administrator are used in this document, these terms are generic and pertain to any person who performs those duties, not just those with that title or primary job duty.

PURPOSE OF THESE REQUIREMENTS

By information security we mean protection of electronic information processed by either a data controller or data processor. The purpose of this document is:

- To establish an industry-wide approach to information security that protects information processed by both data controllers and data processors.
- To reinforce the culture of security and responsibility in organisations that serves to protect individuals and interests.
- To prescribe mechanisms and rules that help identify and prevent the compromise of information security and the misuse of data, networks and computer systems.
- To define mechanisms and rules that will help to protect the reputation of the DM and marketing industry and allow the organisations to satisfy their legal and ethical responsibilities.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with these requirements.

1. GENERAL REQUIREMENTS

The organisation must use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of data, network and system resources.

1.1 The organisations senior management must be involved and informed in the information security process.

1.2 Policies and/or documented processes must be in place to define how the organisation manages information security in all its aspects. At a minimum it must define how the organisation satisfies the requirements set out in these sections:

2. RISK ASSESSMENT
3. MANAGEMENT RESPONSIBILITY
4. TRACEABILITY AND RESPONSIBILITY
5. ACCEPTABLE USE
6. ACCESS CONTROL
7. PASSWORDS
8. VIRUS / SPY PREVENTION
9. INTERNET / NETWORK SECURITY
10. SYSTEM / SERVER SECURITY
11. BACKUPS
12. DATA STORAGE AND ELIMINATION
13. OUTSOURCING
14. EXCEPTIONS

2. RISK ASSESSMENT

2.1 A documented risk assessment process must be undertaken at a minimum annually assessing the probability and impact of threats. When significant changes occur to the business, locations or equipment or after a major security incident an additional review must be undertaken.

2.2 The risk assessment must identify and quantify (estimate) the magnitude of risks relating to data within the organisation. This could include the risks inherent in staff working from home and mobile working.

For guidance, a risk assessment process summary is documented in Appendix 1 which outlines the minimum typical information required.

For additional guidance, a risk assessment template and risk tolerance matrix are also available from the DMA web site at http://www.dma.org.uk/content/risk-assessments

3. MANAGEMENT RESPONSIBILITY

The organisation's management team (MT) is responsible for implementing these requirements.

The MT must ensure that:

3.1 A single named individual has overall responsibility for Information Security and the requirements of this standard. Further staff should be responsible for information security across larger organizations, sites or business sections.

3.2 Each defined business unit has a clear organisation structure and nominated personnel with direct and indirect responsibilities for security implementation, incident response, risk assessments, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

3.3 The organisations information security rules and documentation are reviewed on a periodic basis (minimum annually), are published and available as appropriate.

3.4 All staff must be sufficiently trained to ensure they understand the organisation's information security policies, data sensitivity, confidentiality and relevant aspects of the Data Protection Act. This must be tailored to the role of the individual e.g. network administrator, system administrator, data user and general staff.

Training must commence with a formal documented induction process which must be followed by refresher sessions at a minimum annually or upon significant change to the business or an employee's role. Records of content, attendance and attainment must be maintained.

3.5 Violation of the information security requirement must be recorded and result in disciplinary actions as appropriate and as authorized by the organisation in accordance with defined disciplinary policies, procedures and codes of conduct.

3.6 Members of the MT are each responsible for implementing these requirements within their areas of responsibility, and for monitoring compliance.

4. TRACEABILITY AND RESPONSIBILITY

It is essential that the location and type of all data be known throughout its use in the organisation.

4.1 A record of all data received, stored, processed or sent must be accurately maintained. This must include a clear description of the information, its ownership, purpose and any special security requirements and use restrictions.

4.2 All data must be recorded and protected on receipt.

4.3 All data must be assigned an individual 'owner' on receipt.

4.4 It is the organisation's responsibility to implement the necessary security requirements throughout its use in the organisation.

4.5 The data and its corresponding level of protection must be consistent when the data is replicated and as it is used by the organisation.

It is good practice to keep records for each replicated set of data, recording how it has been used, why and by when.

4.6 All data must be encrypted during transfer, transmission or delivery to third parties or to separate systems outside the direct control of the organisation. Clients may instruct otherwise in which case their instructions must be retained for reference.

Note: Basic free software is available to assist in an encryption processes.

5. ACCEPTABLE USE REQUIREMENT

How staff use information and resources can have dramatic implications on the overall security of the organisation and its data. Rules must be put in place that limit what staff are allowed to do and education provided so they understand good practice.

5.1 Organisation computer resources must be used in a manner that complies with organisation rules and legal requirements.

5.2 Use of organisation computing, networking or facilities by employees must not interfere in any way with the effective running of a organisation's business or the employee's duties.

5.3 Use that interferes with the proper functioning or the ability of others to make use of the organisation's networks, computer systems, applications and data resources are not permitted.

5.4 Use of organisation computer resources for personal profit is not permitted except under specific recorded MT permissions.

5.5 Decryption of passwords, unauthorized access or circumvention of security processes is not permitted, except by authorized staff performing security reviews or investigations. Violations must be formally disciplined and staff may be dismissed in line with organisation policy.

6. ACCESS CONTROL

There is a delicate balance between protecting data and permitting access to those who need to use data for authorised purposes. This balance should be recognised.

6.1 Servers and any information storage medium must have a dedicated owner responsible for both maintenance and use.

6.2 The organisation must have a standard process that applies to user access rights. This will suffice for most instances. Management may enact more restrictive policies for end-user access to data as applicable.

6.3 Access to the network and servers and systems must be achieved by individual and unique logins and must require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognised forms.

6.4 Users must not share authentications. Usernames and passwords must not be written down or recorded in unrestricted media, files or documents.

6.5 All users are responsible for and must secure their authentication, username or account and system access from unauthorized use.

6.6 Network and physical access for visitors to the business premises must be restricted. If guest accounts are present, they must be configured to limit access to named and authorised resources.

6.7 Appropriate measures must be in place to control information access in regard to new or temporary staff.

For guidance, such measures could include induction training for all starters or temporary staff and insuring access to client and customer data is only permitted after training has been successfully completed.

6.8 If additional staff require access to client-related documents or files for legitimate business reasons, limited exceptions are allowed. Each such request must be reviewed by the MT and requires prior and recorded approval.

7. PASSWORDS

Passwords and user authentication are a key security requirement. Proper control, creation and use deliver real benefit when integrated with other controls. Many authentication processes exist; if specific products / tools are used they must meet or exceed the level of security provided by passwords in this section.

7.1 All systems containing or controlling data must have strong authentication or passwords. Passwords must be eight characters or more in length, using a combination of alpha and numeric characters.

7.2 Empowered accounts, such as administrator, root or supervisor accounts, must have such passwords controlled and not distributed widely.

7.3 Standard accounts such as users must have password changes forced, consistent with guidelines established by the organisation. Passwords must not be re-used.

7.4 Passwords must not be placed/distributed in emails or any system where they could be accessed by unauthorised individuals unless they have been protected or encrypted.

7.5 Default passwords on all systems must be changed during installation.

7.6 Logins and passwords must not be remembered, coded or recorded into programs or queries unless they are encrypted or otherwise secure. Where system or hardware passwords must be recorded, restricted access to named individuals via a defined process must be in place.

7.7 Users are responsible for safe handling and storage of all organisation devices. Authentication tokens (such as a SecureID card or tokens) must not be stored with a computer that will be used to access the organisation network or system resources.

7.8 If an authentication device is lost or stolen, the loss must be immediately reported to the MT and an appropriate individual in the issuing unit so that the device can be disabled. This must be traceable and fully documented.

7.9 Employees that have their roles terminated must have their accounts terminated as part of a pre-defined process. Transferred employees must have access rights reviewed and adjusted as found necessary. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews must be conducted by the owners of the systems / information.

8. VIRUS / SPY PREVENTION

This growing threat should be taken extremely seriously by all organisations. Inexpensive and robust solutions are available, however good practice and education is vital.

8.1 The wilful or incompetent introduction of computer viruses or disruptive/destructive programs into the company environment is prohibited; violators must be formally disciplined in line with organisation policy.

8.2 All desktop systems servers and workstations that connect to the network must be individually protected with an approved, licensed anti-virus software and anti-spy product that it is kept updated according to the vendor's recommendations.

8.3 All data both incoming and outgoing including electronic mail must be scanned for viruses and harmful code prior to acceptance or release. It is good practice to have a stand alone machine, not connected to the internal network to do this.

8.4 Infected data intercepted must be destroyed or quarantined automatically. Logs / records must be retained and must be transmitted to the administrator automatically.

8.5 Reports must be produced on the propagation of viruses and the state of the anti-virus software.

8.6 Users must not interfere with the operation of anti-virus software.

8.7 Automatic virus and spyware scans must be used to inspect all servers, workstations and stored data weekly.

9. INTERNET / NETWORK SECURITY

The connectivity used to transfer data can often be easily compromised - both internally and externally.

9.1 All connections to the Internet must go through a firewall secured connection point to ensure the entire network is protected.

9.2 Wireless connections should be configured either with defined Mac addresses or through Wi-Fi Protected Access (WPA) protocol or higher security processes. If Wired Equivalent Privacy (WEP) protocol is used SSID Identifiers must not be broadcast. Wireless access points must be connected to the network via a firewall.

9.3 Physical access to switches and routers must be prevented from unauthorised individuals.

9.4 Alteration or additions to the network must only be performed by authorised persons.

10. SYSTEM / SERVER SECURITY

10.1 All systems connected to the Internet must have a licensed vendor supported version of the operating system installed, up to date and concurrent with usage.

10.2 All systems must be current with security patches / updates, as appropriate. Security patches must be updated at the next opportune installation window.

Ideally mission critical servers should be updated within 24 hours from the release of vendor security patches.

10.3 All software installed must be licensed, up to date and concurrent with usage.

10.4 Applications or executable code must not be used or installed without documented authorisation.

10.5 An accurate record of system builds and authorisation must be maintained.

11. BACKUPS

Backing up of data is a necessity in any IT infrastructure. Special care should be taken in getting the details correct as minor faults or incorrect settings could invalidate the process.

11.1 All data must be backed up on receipt. Legitimate exceptions must be retained for reference.

11.2 All back-ups stored or transferred to third parties or to separate systems outside the direct control of the organisation must be encrypted.

11.3 The regularity of back-ups must reflect the value of the data. Back-up frequency may differ depending on the nature of the data held.

11.4 Back-ups must be well documented with validation logs kept and reviewed to ensure that back-ups were successful or to highlight faults.

11.5 Back-ups must be tested periodically (minimum twice per year) and documented to ensure their quality.

11.6 Back-ups must be securely stored both on and off site. It is good practice to keep spare back-up media onsite for emergencies.

11.7 Data must be kept for no longer than necessary, in accordance with the Data Protection Act 1998. Organisations' policies / agreements with data controllers which dictate durations / purging cycles should be retained for reference.

11.8 As a minimum back-ups of data must be handled with the same security precautions as the data itself.

11.9 Complete back-ups must be kept offsite. If a third party is involved a contractual agreement must be in place between the offsite storage facility and the business. Any back-up data kept onsite must be kept in a secure and purpose designed fireproof 'data' container - with only back-up administrators and/or authorized staff having access.

11.10 How back-ups are returned both in rotation and in emergencies must be pre-defined.

12 DATA STORAGE AND ELIMINATION

Once information has been used for the defined purposes it can be deleted. The deletion of information is good practice as it reduces the volume of information controlled and backed up. However due care should be taken to delete the right information and to ensure it has been completely removed.

12.1 Version control and ownership of data must be maintained.

12.2 After completion of designated tasks, user copies must be deleted or access removed as appropriate.

12.3 Surplus computers, drives or media must be treated with caution. All customer data must be overwritten as to make the data unrecoverable or have the media removed and or destroyed prior to disposal.

12.4 Records must be kept of all disposals of media and systems. This must include approvals, destination, payments and facilitating parties.

12.5 Records of progress and actions must be maintained. Documents or tags that clarify actions/ progress taken must be affixed to the body of the computers, drives or media if uncompleted.

12.6 Print waste, printouts or materials containing data must be rendered illegible, destroyed prior to removal or removed via a secure carrier.

Note: normal Windows / Mac 'delete' is not adequate if the computer or media is being disposed of or being re-used for a non secure purpose. Basic free software is available to assist in data removal processes.

13. OUTSOURCING

13.1 When data is transferred from one organisational entity to another, contracts between the two parties must include requirements for the security of data and service levels. These will include access controls to meet all the requirements in sections 3 - 12 of this standard.

13.2 The organisation must monitor data processors to ensure requirements for security are implemented. This may include audits or reliance on their external security qualification such as ISO 27001 or DMA DataSeal.

13.3 All data transmitted to and from the supplier must be encrypted. This maybe implemented through file encryption, encrypted transmission or using secure FTP.

13.4 Where there are interconnections to a data processor's information systems, controls must be implemented to ensure compliance with sections 1 - 12 of this standard.

14. EXCEPTIONS

In certain cases, compliance with specific requirement requirements may not be immediately possible. Reasons include, but are not limited to, the following:

14.1 Required commercial or other software in use is not currently able to support the required features.

14.2 Legacy systems are used that do not comply, but near-term future systems will, and are planned for.

14.3 Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, a written explanation of the compliance issue and a plan for coming into compliance with this Information Security Requirement in a reasonable amount of time must be produced. Explanations and plans must be submitted to the MT and recorded. This must be traceable and fully documented. Details of non-compliance must be reported to the DMA via compliance@dma.org.uk and will be reviewed and approved on an individual basis.

This document was produced by the DMA and came into effect on 27 January 2012.

This document provides a specification for use by internal and external parties, to assess the organisation's ability to deliver basic data security. It does not replace, supersede or meet those higher requirements found in ISO 27001.

Auditing of a successful implementation of this document can be used by an organization to demonstrate to interested parties that functional data security process are in place.

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with this document cannot confer immunity from legal obligations.

The DMA would like to thank Terry Heimbaugh of 'The University of Illinois', Mike Softley of Ultima and Peter Galdies of DQM for their generous support in preparing this document.

Certification / Auditing

Information on auditing and certification to this scheme can be obtained from: compliance@dma.co.uk

Revisions

This document will be updated by amendment or revision. Users of this document should make sure that they possess the latest amendments or editions.

Copyright

APPENDIX 1

Risk Assessment Process

The organisation must undertake a documented Risk Assessment at a minimum annually or upon any significant change(s) to the business. This process must typically include the following as a minimum to ensure compliance with the DataSeal standard.

Risk Description and Analysis

By assessing the inherent probability and impact of each risk the organisation must identify and quantify (estimate) the magnitude of risks relating to client data within the organisation.

Risk Criteria

The organisation must establish clearly defined rules for the acceptance of risks. This must stipulate the level of risks which are unacceptable to the organisation and the basis for any exceptions. Exceptions should only be based on those exceptions referred to in Section 13 of this standard.

Risk Evaluation

The risk evaluation is the process of comparing those risks identified in the risk analysis to the risk criteria established. This process may be integrated into a risk analysis template. Having undertaken the comparison the organisation must produce a risk treatment plan.

Risk Treatment Plan

For each risk identified through the risk evaluation process the organisation must identify the appropriate the risk treatment.

This process demonstrates how risks are mitigated to ensure that they are acceptable to the organisation based on the risk criteria.

Risks can be mitigated in one of four ways:

- Reduce: the organisation will implement additional controls to mitigate the risk. These should be documented.
- Acceptance: the organisations management accept the level of risk based on the risk criteria. Acceptance of the risk assessment is often demonstrated through documentation in the minutes of a meeting
- Avoid: the organisation decides not to undertake the activity due to the risks involved.
- Transfer: the organisation mitigates the risk by transferring the risk to a third party.