Department of Military Affairs

Data Classification/Protection Policy

Andrew C Quist

1 Overview

1.1 Department of Military Affair's (hereby referred to as DMA) intentions for publishing an Data Classification Policy are not to impose restrictions that are contrary to DMA's established culture of openness, trust and integrity. We are committed to protecting DMA's employees, partners and the department from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.2 DMA Data is information generated by or for, owned by, or otherwise in the possession of DMA that is related to the DMA's activities. DMA Data may exist in any format (i.e. electronic, paper) and includes, t is not limited to, all academic, administrative, and research data, as well as the computing infrastructure and program code that supports the business of DMA.

1.3 In order to effectively secure DMA Data, we must have a vocabulary that we can use to describe the data and quantify the amount of protection required. This policy defines four categories into which all DMA Data can be divided:

1.3.1 Public

1.3.2 Internal

1.3.3 Confidential

1.3.4 Restricted Use

1.4 DMA Data that is classified as Public may be disclosed to any person regardless of their affiliation with the DMA. All other DMA Data is considered Sensitive Information and must be protected appropriately. This document provides definitions for and examples of each of the four categories. Other policies within the Data Protection Standards specify the security controls that are required for each category of data.

1.5 The various units and divisions at the DMA have a multitude of types of documents and data. To the extent particular documents or data types are not explicitly addressed within this policy, each business unit or department should classify its data by considering the potential for harm to individuals or the DMA in the event of unintended disclosure, modification, or loss. The CIO may assist with the classification process and coordinate with the Information Security Team to achieve consistency across the DMA. When classifying data, each department should weigh the risk created by an unintended disclosure, modification or loss against the need to encourage open discussion, improve efficiency and further the DMA's goals of the creation and dissemination of knowledge. Divisions should be particularly mindful to protect sensitive personal information, such as Social Security Numbers, drivers' license numbers and financial account numbers, disclosure of which may create the risk of identity theft.

1.6 Some information could be classified differently at different times. For example, information that was once considered to be Confidential data may become Public data once it has been appropriately disclosed. Everyone with access to DMA Data should exercise good judgment in handling sensitive information and seek guidance from management as needed.

2 Scope

2.1 This classification scheme is to be applied to all DMA Data, both physical and electronic, throughout DMA. No data item is too small to be classified. This policy applies to employees, contractors, consultants, temporaries, and other workers at DMA, including all personnel affiliated with third parties. This policy applies to all equipment that is owned, leased, or personal machines(After Personal use document is signed) by DMA.

3 Classification Levels

3.1 Public

3.1.1 Public data is information that may be disclosed to any person regardless of their affiliation with the DMA. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the DMA community and no steps need be taken to prevent its distribution.

3.1.2 Examples of Public data include: press releases, directory information (not subject to a Family Educational Rights and Privacy Act (FERPA) block), course catalogs, application and request forms, protected health information that has been de-identified consistent with the standards set forth under Health Insurance Portability and Accountability Act (HIPAA), and other general information that is openly shared. The type of information a department would choose to post on its website is a good example of Public data.

4 Internal

4.1 Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data generally should not be disclosed outside of the DMA without the permission of the person or group that created the data. It is the responsibility of the data owner to designate information as Internal where appropriate. If you have questions about whether information is Internal or how to treat Internal data, you should talk to your department head.

4.1.1 Examples of Internal data include: Some memos, correspondence, and meeting minutes; contact lists that contain information that is not publicly available; and procedural documentation that should remain private.

5 Confidential

5.1 Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or the business of DMA. This classification also includes data that the DMA is required to keep confidential, either by law (e.g., FERPA) or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported.

5.1.1 Any unauthorized disclosure or loss of Confidential data must be reported to the Information Systems Support Incident Response Team at 406-324-3337 or dmatech@montanadma.org.

5.1.2 Examples of Confidential data include:

5.1.2.1 Information covered by the Family Educational Rights and Privacy Act (FERPA), which requires protection of records for current and former students. This includes pictures of students kept for official purposes.

5.1.2.2 Personally identifiable information entrusted to our care that is not otherwise categorized as Restricted Use data, such as information regarding applicants, alumni, donors, potential donors, or parents of current or former students.

5.1.2.3 The DMA ID Number, when stored with other identifiable information such as name or e-mail address.

5.1.2.4 Information covered by the Gramm-Leach-Bliley Act (GLB), which requires protection of certain financial records.

5.1.2.5 Individual employment information, including salary, benefits and performance appraisals for current, former, and prospective employees.

5.1.2.6 Legally privileged information.

5.1.2.7 Information that is the subject of a confidentiality agreement.

5.1.2.8 Information that is the subject of a HIPAA Limited Data Set covered by a Data Use Agreement.

6 Restricted Use

6.1 Restricted Use data includes any information that has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require the DMA to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual.

6.2 The DMA's obligations will depend on the particular data and the relevant contract or laws. The Minimum Security Standards sets a baseline for all Restricted Use data. Systems and processes protecting the following types of data need to meet that baseline:

6.3 Personally Identifiable Information (PII) including an individual's name plus the individual's Social Security Number, driver's license number, or a financial account number.

6.4 Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens.

6.5 "Criminal Background Data" that might be collected as part of an application form or a background check.

6.6 More stringent requirements exist for some types of Restricted Use data. Individuals working with the following types of data must follow the DMA policies governing those types of data and consult with Information Security to ensure they meet all of the requirements of their data type:

6.7 Protected Health Information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA).

6.8 Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored.

6.9 Controlled Unclassified Information required to be compliant with NIST 800.171

6.10 Data controlled by U.S. Export Control Law such as the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). ITAR and EAR have additional requirements.

6.11 U.S. Government Classified Data

6.12 Restricted Use data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure, unauthorized modification, or loss of Restricted Use data must be reported to the Incident Response Team at 406-324-3337 or dmatech@montanadma.org.

7 Resolving Conflicts between this Guideline and Other Regulations

7.1 Some data may be subject to specific protection requirements under a contract or grant, or according to a law or regulation not described here. In those circumstances, the most restrictive protection requirements should apply. If you have questions, please contact Information System Support.

8 Important

8.1 Failure to comply with the Data Protection Standards may result in harm to individuals, organizations or DMA. The unauthorized or unacceptable use of DMA Data, including the failure to comply with these standards, constitutes a violation of DMA policy and may subject the User to revocation of the privilege to use DMA Data or Information Technology or disciplinary action, up to and including termination of employment.

9 Policy Compliance

9.1 Compliance Measurement

9.1.1 The DMA team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

9.2 Exceptions

9.2.1 Any exception to the policy must be approved by the DMA team in advance.

9.3 Non-Compliance

9.3.1 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10 Related Standards, Policies and Processes

Data Protection Standard

Social Media Policy

Minimum Access Policy

Password Policy

Definitions and Terms

Blogging

Honeypot

Honeynet

Proprietary Information

Spam

Revision History

Date of Change	Responsible	Summary of Change
Sept 2015	Information Support Section	Updated and converted to new format