INFORMATION CLASSIFICATION & EXCHANGE POLICY		
Doc. ID: IT-P-010	**Version:** 3.0	**Effective Date:** 10-Apr-2017
Owner: Chief Information Officer		

1. TABLE OF CONTENTS

2. PURPOSE & SCOPE

The purpose of this policy is to classify MMS Holding Inc (MMS) business information to ensure the appropriate level of security and protection during information receipt, exchange, and disposition. This policy is applicable to all information/data exchanged between MMS and any external party.

Classified information/data includes confidential, proprietary, and private as defined within this policy. Details specific to management of each classification type are defined in the tables in Section 4.

Any violation of this policy will be reviewed by the Senior Leadership Team for determination of corrective and/or disciplinary actions as required.

3. TERMS, ACRONYMS, & REFERENCES

Refer to the MMS Global Glossary for terms and acronyms; referenced documents are linked within.

- Refer to the Protection of Private Information WP (QA-WP-001) for details on protecting Private Information (PI), and the process for management of PI disclosure.
- Refer to the Document Control SOP (QA-SOP-001) and the Record Control SOP (QA-SOP-004) for more details on document owners and document and record management.
- Refer to the Access Control Policy (IT-P-016) for details on MMS access provisions. Access is limited to permitted individuals as defined within IT-P-016.

4. POLICY DETAILS

4.1 COLLEAGUE AWARENESS & CONFIDENTIALITY AGREEMENT

4.1.1 All colleagues are made aware of the importance of maintaining confidentiality of classified information/data upon hiring and provided at least annual refresher training.

4.1.2 When employment begins, each colleague is required to sign a Confidentiality Agreement that includes a provision requiring the colleague to maintain confidentiality of classified information.

4.1.3 Post-Employment Re-Commitment - Upon termination of employment, an exit interview will be conducted with each colleague. During the exit interview, the colleague will be reminded of their ongoing contractual obligation under the company Confidentiality Agreement.

4.2 INFORMATION AND DATA EXCHANGE

4.2.1 Client/project information and data must be exchanged following client requirements for that specific project; details of permissible exchange methods (e.g., email, drop box, eShare, client system, etc.) are documented in PWA.

4.2.2 Emailing classified information/data to a personal email account or any non-permitted recipient is strictly prohibited.

4.2.3 Faxes and emails containing classified information should include a message or cover page indicating classification, and that it is intended for the marked recipient(s) only, for example:

> Note: The information contained in this message may be privileged and confidential, and thus protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by reply to the fax number and shred the same. Thank you

4.2.4 Shipping of classified information/data is only completed as requested by and per client specifications using tamper evident packaging.

4.3 INFORMATION AND DATA SAFEGUARDS

4.3.1 Do not leave classified information/data out in the open or in common areas.

4.3.2 Do not discuss classified information/data in public or with any unauthorized personnel.

4.3.3 Ensure classified information/data is always stored and locked in designated drawers/cabinets and keys are kept secure.

4.3.4 Always lock your computer when unattended and never share log-in credentials.

4.3.5 Ensure that emails are sent only to permitted and intended recipients (double check email addresses prior to sending).

4.3.6 Encrypt files with a password when required and communicate the password in a secure, separate, and private communication.

4.4 CONFIDENTIAL INFORMATION AND DATA MANAGEMENT

Definition	Confidential information and data is anything considered to be vital to MMS and/or our clients, and is not generally known outside of MMS business interactions. Release of confidential information outside of MMS is only permitted per client contract or with permission from the Vice President, Chief Information Officer, or Sr. Manager, Corporate Quality & Information Systems.
Examples	• Client provided documents, details, product data, study results, etc.; • MMS generated documents and deliverables; • IMS documents and records; • MMS and client training materials and records; and • MMS and client templates, forms, guidances and guidelines.

Function	Process Requirements
Saving & Storage	• Client provided data/information may only be stored on removable media (e.g., zip drive, USB storage device, compact disc, etc.) if permitted by client agreement(s), and only for the purpose of the project. • Removeable media must only contain data/information for the specific client/project and must be permanently erased, securely archived, returned to the client, or destroyed once no longer needed, based on client preference. • Storage within the client's systems must comply with client processes. • Storage and archiving within MMS systems must comply with the Document Control SOP (QA-SOP-001) and the Record Control SOP (QA-SOP-004). • Storage/saving on personal computers is not permitted. Temporary files saved to work computers must be permanently deleted when no longer needed.
Printing	• Printing of client provided information/data is allowed only if permitted by the client and only for the purposes of the project. • Whenever possible, avoid printing confidential information, but when required, mark each page as 'confidential' (e.g., stamp or watermark tool). • Utilize the secure print option where available and required. • Retrieve printed documents immediately. • When no longer needed, printed documents are to be permanently destroyed (deposited in the shredding bins, or personally shredded by the colleague).
Distribution & Communication	• Confidential information is not communicated, shared, or distributed in any manner outside of the intended recipients (e.g., MMS colleagues and project team, client project team, etc.).

4.5 PROPRIETARY INFORMATION AND DATA MANAGEMENT

Definition	Proprietary information is information of financial nature related to MMS. This information is only available for viewing by permitted MMS staff. Release of proprietary information to unauthorized personnel within MMS, or outside of MMS can only be done with authorization from the Vice President, Chief Financial Officer, or Executive Director, Project and Account Management.
Examples	• Quotes, costs, hourly rate, balance sheets, and expense runs.

Function	Process Requirements
Saving & Storage	• Proprietary information is not permitted to be saved/stored either on removeable media or outside of the originating location unless specifically permitted by the client or MMS Document Owner. • Printed documents are stored in designated locked cabinets/drawers.
Printing	• Whenever possible, avoid printing proprietary information. • Personnel with access to print proprietary information must print using private printers provided. In extreme cases printing to common printers is permitted but documents must be collected immediately and personally, and should be marked as 'proprietary' (e.g., stamp or watermark tool). • When no longer needed, printed documents are to be permanently destroyed (deposited in the shredding bins, or personally shredded by the colleague).
Distribution & Communication	• Proprietary information can be distributed and communicated only to permitted MMS personnel, and to clients where contractually agreed.

4.6 PRIVATE INFORMATION AND DATA MANAGEMENT

Definition	Private Information (PI) includes: Protected Health Information (PHI), Personally Identifiable Information (PII), Sensitive Personal Information (SPI), personal financial/billing information, restricted data, or any information considered to be private by MMS, the client/project requirements, and/or applicable local data privacy laws and regulations. Refer to the Protection of Private Information WP (QA-WP-001) for more details.
Examples	• Personal descriptors, e.g., name, age, place of birth, date of birth, gender, weight, height, eye color, hair color, fingerprint or other biometric identifiers; • Identification numbers, e.g., Health IDs, Social Insurance Numbers, Social Security Numbers, National Insurance Numbers, Personal Identification Number (PIN), debit or credit card numbers, banking numbers, etc.; • Ethnicity, e.g., race, color, nationality, or ethnic origin; • Health information, including genetic information; • Personal billing/financial, and employment information; and • Other MMS, client/project, or external party-defined PI.

Function	Process Requirements
Saving & Storage	• Private information/data is not permitted to be saved/stored on removeable media or outside of the originating location unless specifically permitted by the client or in an agreement between all stakeholders. • Printed documents are stored in designated locked cabinets/drawers.
Printing	• Whenever possible, avoid printing private information/data. • Permitted personnel must print using private printers provided. In extreme cases printing to common printers is permitted, but documents must be collected immediately and personally, and marked as 'private' (e.g., stamp or watermark tool). • When no longer needed, printed documents are to be permanently destroyed (deposited in the shredding bins, or personally shredded by the colleague).
Distribution & Communication	• Distribution and communication of MMS private information/data is restricted to document owners and permitted personnel only. • External release of client-provided private information/data is only permitted per contractual agreement between applicable stakeholders.

5. METRICS

NA

6. AMENDMENT RECORD

Version	Date	Description of Changes
0.0	09-Sep-2009	New Document Release.
1.0	12-May-2010	Clear desk practices added.
2.0	10-Jun-2011	PHI management added.
3.0	10-Apr-2017	Moved to new template, merged P-IT-009 Information Classification Policy into this policy and renamed as IT-P-010 Information Classification and Exchange Policy (prev. Information Exchange Policy). PHI expanded to include all types of PI. Clarifications and details added throughout.

7. REVIEW AND APPROVAL

If the Document Owner is the Quality Manager, a separate Quality Assurance designee or member of the Senior Leadership Team may sign as the Quality Assurance Approver.

	DOCUMENT OWNER APPROVAL	QUALITY ASSURANCE APPROVAL
NAME, TITLE:	Mohamad Zahreddine Chief Information Officer	Jessica Alamdari Process Improvement Specialist
SIGNATURE, DATE:	DocuSigned by: Mohamad Zahreddine Signer Name: Mohamad Zahreddine Signing Reason: I approve this document Signing Time: 2017-04-06 20:50:15Z (UTC) 873AA6E7FC4F453094E1F0D3D13F2DC1	DocuSigned by: Jessica Alamdari Signer Name: Jessica Alamdari Signing Reason: I approve this document Signing Time: 2017-04-06 20:49:01Z (UTC) 6DD9B8F88F884577B3242C8A7F9A3A05