Data & Information Technology Management Standard

Reference No	: OPT-M-2016-010
Version	: 1.0
Release Date	: 10 April 2016
Author	: KU KA TONG
Approval	: XIAO ZHIJUN
Use	: Private

Revision History

Version	Date	Description	Prepared by
1.0	10 Apr 2016	Initial Release	Ku Ka Tong

Contents

1. Introduction

What is Data & Information Management?

Information Management is the means through which the organization ensures that the value of its information resources is identified so that these resources may be utilized to their fullest potential. The primary objective of IM is to ensure that the right information is available to the right person, in the right format at the right time. IM is the way in which an organization plans, identifies, captures, manages, preserves and disposes of its information across all formats, (physical and digital), and includes the management of all functions associated with information, such as security, metadata management, quality management, etc.

Why is Information Management important?

Company ability to respond to the needs of our operation depends on how well it can create, use and preserve information to make decisions and take action to achieve its operational and strategic goals. Along with people and finances, information is a key business resource for the company, and as such, the management of that information is critical to achieving the government's priorities.

Data & information management is a cycle of a company activity: the acquisition of data & information from one or more sources, the custodianship and the distribution of that data & information to those who need it, and its ultimate disposition through archiving or deletion. This cycle of company involvement with data & information involves a variety of stakeholders: for example those who are responsible for assuring the quality, accessibility and utility of acquired data & information, those who are responsible for its safe storage and disposal, and those who need it for decision making. Stakeholders might have rights to originate, change, distribute or delete data & information according to company data & information management policies.

Data & information management embraces all the generic concepts of management, including: planning, organizing, structuring, processing, controlling, evaluation and reporting of data & information activities, all of which is needed in order to meet the needs of those with company roles or functions that depend on data & information. Data & information management is closely related to, and overlaps, the management of data, systems, technology, processes and – where the availability of data & information is critical to company success – strategy. This broad view of the realm of data & information management contrasts with the earlier, more traditional view, that the life cycle of managing data & information is an operational matter that requires specific procedures, company capabilities and standards that deal with data & information as a product or a service.

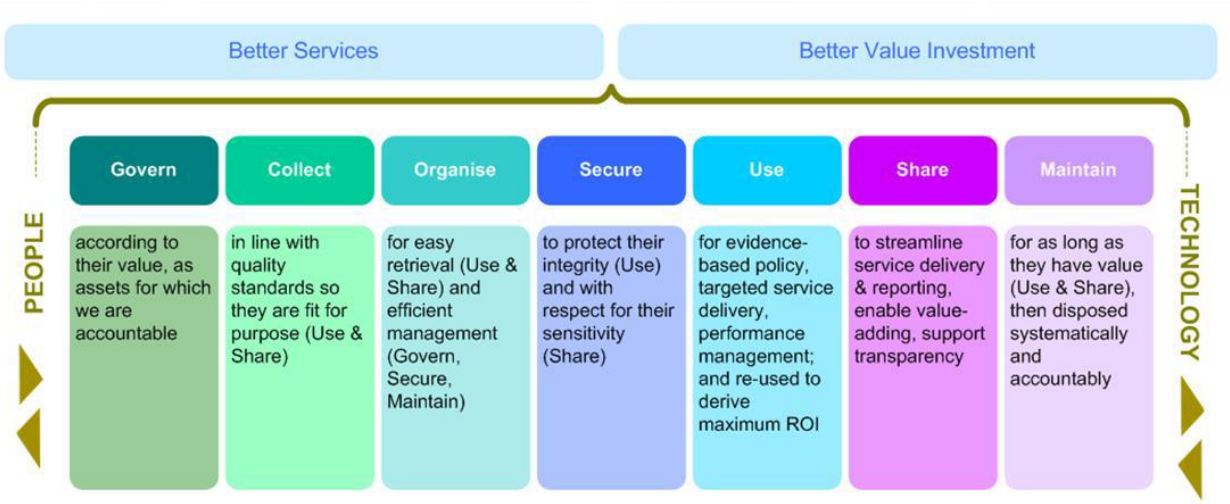
A company ability to process data & information is at the core of organization and managerial competency, and an organization's strategies must be designed to improve data & information processing capability and

as data & information systems that provide that capability became formalized and automated, competencies were severely tested at many levels.

The goal of information management is to enable company organization to control and administer information assets throughout their life-cycle– that is, to capture, distribute, use, maintain and dispose of data and information in a secure, efficient and accountable manner.

By considering the desired outcomes across all stages of the cycle, data and information can be managed in support of better service delivery and better value investment.

Figure below illustrates the outcomes-based approach to information management:



The objectives of this standard are to:

- Provide guidance for key legislation, including but not limited to
  - Document transfer and disposal
  - Electronic Documents & Transactions
  - Company & Personal Data & information Protection
- Define authorities, responsibilities and accountabilities for data & information and technology management.
- Provide a policy framework within which company can derive the maximum benefits from the use of data & information and technology.
- Establish policies for the management of data & information and technology activities.
- Establish a database management of company data & information management.
- Increase the company efficiency in all aspect of management process.

2. Principles

Given the business value generated from information, and the long-term value of the company's information holdings, it is important that we define a vision for information management in the organization.

INFORMATION IS:

COLLECTED ONCE;

MANAGED DIGITALLY IN AN

OPEN AND SECURE

ENVIRONMENT;

ACCESSIBLE;

AND

USED TO ITS

FULLEST POTENTIAL.

Data & information management is a core component of company infrastructure; it is the intellectual capital of responsible governance. Best practice policies and standards result in efficient, accountable and cost-effective use of resources. Data & information constitutes the full spectrum of technologies and services that support data & information management. The principles underlying effective management are:

- Data & information is a vital company asset that must be managed and, where appropriate, shared to maximize investments;
- Data & information are key components in delivering cost-effective company services to the client;
- Data & information have the potential, when planned and managed properly, to improve productivity and reduce costs to company;
- Data & information and technology are strategic enablers of quality company service delivery;
- Others company management standards also apply to data & information and technology resources.

3. Scope

People: Applicable to all OPT locations, including but not limited to whole own company, subsidiaries and/or joint venture company where permits. All employee must follow this standard.

- Areas of Interest: Applicable to all OPT related information transaction &activities and documents such as (but not limited to) the following :

- Company legal and Financial data & Information
- Employee Data& Information
- Contract & Agreement
- Laboratory Process and Data
- Equipment & Maintenance Information
- Product Research Information and Data Sheet
- Quality & HSE data & information
- Job Proposal , Execution Report & Post Job Report
- Marketing & Sale & Data
- Email data & Information communication
- Social Media communication

4. Exemptions

Any deviation from this and other relevant OPT Standard is by exemption only. Due to its sensitivity, the exemptions must be approved by President and above position to approve the exemption. Should the exemption(s) is/are deem appropriate and happen frequently, a new version of the standard should be made and announce by President and above positions.

5. Responsibilities

IT Committee/Director - The IT Committee has ultimate accountability for the implementation of the system and infrastructure plan, and work with key stakeholders to ensure that the actions are completed. The IM Directors across the GoA will work under the direction and guidance of the IT Committee and collaboratively with the all users to achieve the specific projects and deliverable to achieve objectives. It also responsible for training the employee in using these system.

Line Managers – Ensure full compliance with this standard; Ensure all personnel received training; Ensure appropriate resources if any to comply with this standard. Approved exemption if any. Assign responsibility and accountability for the management of information within the custody, or under the control of company management team. Assure compliance with legislation, policies and standards.

Create and retain a full and accurate record documenting decisions and actions. Provide relevant information in a timely, useable, cost-effective, and accurate manner.

Preserve confidential and critical information in a manner that retains the information's authenticity, reliability, accessibility and integrity for as long as required.

Support transparent and effective access to company information within legally established privacy and confidentiality restrictions.

Sales and Support Personnel – Knowing and understand this standard; Ensure all reports and other type of documents is compliant with this standard; Ensure customer is properly informed and aware of the any changes in the documents format; recognized the important of company brand and take appropriate

action(s) should any internal employee violate this standard. Provide relevant information in a timely, useable, cost-effective, and accurate manner.

Job Supervisor and others – Ensure all job reports and form are compliant to this standard; recognized the important of company brand and take appropriate action(s) should any internal employee violate this standard. Provide relevant information in a timely, useable, cost-effective, and accurate manner.

6. Implementation

This standard is in parallel with the company's security and information security policy and others management standards.

- OPT-M-2016-002 Corporate Image & Communication Management Standard
- OPT-M-2016-003 Administrative Management Standard
- OPT-M-2016-004 Human Resource Management Standard
- OPT-M-2016-005 Salary Management Standard
- OPT-M-2016-006 Accounting & Finance management Standard
- OPT-M-2016-007 Asset Management Standard
- OPT-M-2016-008 Procurement & Contractor Management Standard
- OPT-M-2016-009 Warehousing & Logistic Standard

6.1 Golden Rules

- Protect your hardware from theft at all times. Lock properly when unattended.
- Classify data and handle data properly.
- Always setup password for folder and files that is confidential.
- Protect data with secure screen savers, encryption or passwords.
- Ensure anti-virus and patches are current.
- Back up your working files frequently.
- Use licensed software only.
- Do not share files or folder in network.
- Use of Non-Business related OPT email address is prohibited. Use of personal email for OPT business is also prohibited.
- Properly dispose of removable media when data is not needed anymore or hardware malfunction.
- Report IT security breach and incidents.

6.2 IT Hardware and Data Protection

The data & information hardware definition includes the Sever, Cloud System, Laptop, Desktop, Storage device, CD or DVD, USB memory stick, and etc. that allowed data or information to be stored.

The data & information hardware management definition including hardware purchasing, security setting, installation, data maintenance, storage and disposal, etc.

All users of company IT resources such as must take responsibility for, and accept the duty to, actively protect them. The hardware/device must be properly secured and locked in place when it is not used. Improper protection of IT hardware may jeopardize the confidentiality, integrity and availability of company information and information technology assets, and may put personal information protection, security or service levels at risk.

When traveling, employee must make sure the laptop/data devices must be kept with him/her all the time. When check in hotel and need to leave the device in the room, it must be properly secure with cable lock or lock in the safety box.

During meeting or client presentation, be aware that the clients maybe request a copy of the data. Please make sure you aware of the classification of the data they are asking. If the data is deem confidential and for reference only, please do reject the request politely. If the data is public and not confidential, we should always provide the copy in PDF format.

In any circumstance, no one is allowed to excess to your laptop or computer unless permission is given by user. Non-OPT employee is prohibited from accessing or using the company electronic devices.

Back-up data frequently into separate storage device or in the company server.

Any loss of the IT hardware must be reported immediately via OPTiSAFE system and to his/her immediate manager. An investigation may be carried out. If there is any loss of the company hardware or devices due to negligence of the employee, disciplinary action may be taken to have the employee to replace the device and termination of employment if the loss if substantial.

6.3 Software Management

Software definition refers to all programs installed in all electronic devices that belong to company asset that operates in such manner to manage the day to day business.

Only licensed software is allowed to be used in the company. Any use of pirated copy used in the PC or Laptop or any other Mobile devices which contains company information may subject to his/her personal liability. The company will not be responsible for any legal liability for employee in case of using illegal software.

Be aware of not to use shareware that the source was not clearly known. If doubt, kindly consult the upper management and/or do own research via trust able forum discussion.

Avoid running any executable file from stranger or friends email attachment.

New virus developed almost every day. Always keep your anti-virus updated with latest security patch. Few recommended free anti-virus software are:

- 360 Total Security https://www.360totalsecurity.com/
- McAfee www.mcafee.com/
- Norton www.norton.com

6.4 Data Protection

Data & Information shall be obtained only for specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. In practice, the data protection principle means that you must:

- be clear from the outset about why you are collecting the data and what you intend to do with it;
- comply with the company policies and standard;
- comply with what the client confidentiality terms and conditions;
- Ensure that if you wish to use or disclose the data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair and not breaching any rules & regulations.

Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- take reasonable steps to ensure the accuracy of any data you obtain;
- ensure that the source of data is clear and authorized;
- carefully consider any challenges to the accuracy of information;
- Consider whether it is necessary to update the information.

Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. In practice, it means that you will need to:

- review the length of time you keep data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; an
- Update, archive or securely delete information if it goes out of date.

Data shall be processed in accordance with the rights of data subjects only. For example, Financial Data should be kept within the company upper management and not be transferred to public or authorized

employee. Technical information must be kept within the respective department only because the sensitivity and confidential.

6.5 Personal Information Protection

Personal data shall be obtained and/or processed fairly and lawfully and, in particular, shall not be processed unless it is requirement by the relevant administrative management and/or governing body of the country we operate. In practice, it means that you must:

- have legitimate grounds for collecting and using the personal data;
- don't use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data with reasonably expectation ;
- Make sure you do not do anything unlawful with the data.

6.6 Email Information

Your use of the company email services must comply with all applicable Laws. This includes laws applicable to you and also policy applicable to OPT and the recipient each Email. Examples of applicable laws include laws relating to spam or unsolicited commercial email (UCE), privacy, security, obscenity, defamation, intellectual property, pornography, terrorism, homeland security, gambling, child protection, and other applicable laws. It is your responsibility to know and understand the laws applicable to your use of the Services and the Emails you generate and send through the services.

NEVER use personal email for Company Business. Wise verse, never use Company email for personal purposes.

All other employee are prohibited to send email on other people behave.

Except the Personnel Department and CEO announcement or newsletter, NEVER send email to non-specific address for everyone in the company. (e.g., webmaster@domain.com or info@domain.com).

Sending Emails that result in an unacceptable number of spam or UCE complaints (even if the Emails themselves are not actually spam or UCE) is prohibited.

Forbidden to forward outsider email such as "junk mail" , "chain letters" , "pyramid schemes", incentives (e.g., coupons, discounts, awards, or other incentives) or other material in any Email that encourages a recipient to forward the Email to another recipient.

All email should have a signature containing the following information:

- Name of the sender;

- Contact Number;
- Disclaimer information in case the email was sent unintentionally to wrong person.

7. Monitoring

The ongoing measurement of performance is critical to ensuring that our information resources are being managed appropriately. As such, one of the priorities will be the development of a performance management framework for across the company. All management personal should be given respective objective for IM audit. This will allow regular assessments of Information Management policies, and procedures, which will not only guide IM practice, but will also serve to inform the need for ongoing revision to the strategy, tactical plans, and to our policy instruments.

It is a responsibility of all OPT employee worldwide to adhere to this standard format. Employees are responsible to ensure that the items defined in this manual are use accurately and kept up-to-date of any new version at all times.

All Supervisor and Managers shall:

- Ensure that all relevant personnel are informed and trained on this standard.
- Provide visible leadership and management commitment to the use of the Company Image, including maintaining their day-to-day communication material and lead by example.
- Conduct formal reviews of the standard with their direct reports occasionally.
- Recognize and reward performers of using the standard.
- Audit compliance with this Standard

All senior managers shall demonstrate their leadership and management commitment to this standard and monitor this for 12 months. Failing to adhere to company Image Standard should be given warning and penalty if his/her unwillingness pro-long for 6 months.