DATA CLASSIFICATION AND MANAGEMENT POLICY

1 DATA CLASSIFICATION

Definitions

1.1 Data is defined as any information within the purview of the International Maritime Organization, including, but not limited to, personnel data, financial data (budget and payroll), divisional/sectional data, legal files, research data, proprietary data, and all other data acquired and retained in any form that pertains to, or supports, the work of the Organization.

1.2 Electronic information resources include, networks, computers, and other devices that store or display data, communications and transmission devices, and software used on such devices.

Classification of data

1.3 Classification is a method of assigning a level of sensitivity to each datum. It helps to determine the extent to which data need to be controlled and secured, including the appropriate electronic information resource in which such data may be stored or other storage methods, if applicable.

1.4 This classification is essential to differentiate between non-sensitive and sensitive or confidential data. All data should be appropriately classified at the time of creation to determine the level of protection that is required.

1.5 A basic system of classification is as follows:

.1 **NS – Non-Sensitive (Public Data)**
Non-Sensitive data is any data that may or must be made available to the general public, with no legal restrictions on its access or use. Examples of NS include, but not limited to:

1.1 information on IMO Public website;

1.2 financial statement of the Organization;

1.3 information available on the public modules of IMODOCS, GISIS; and

1.4 IMO's information on Facebook, Twitter, Flickr, Tumblr and YouTube.

.2 **MS – Moderately Sensitive (Internal/Official Use Only Data)**
Moderately Sensitive data is classified as internal/official data that when disclosed, altered or destroyed, without authorization, could result in an identifiable level of risk to the Organization or others. By default, any data or information system not classified as Highly Sensitive or Non-Sensitive should be treated as MS. MS data include, but not limited to:

.2.1 human resource information such as salary and benefits information;

.2.2 unpublished documents, emails, memos, financial, strategic and business plans;

.2.3 information on security systems;

.2.4 internal operation procedures, manuals, floor plans; and

.2.5 draft meeting documents, reports or submissions by a Member State.

.3 **HS – Highly Sensitive (Confidential/Sensitive Data)**
Highly Sensitive data is any data which, if released could significantly impact the personal privacy of an IMO delegate or employee, or data that, if released, could have a significant negative impact on bi-lateral or multilateral negotiations occurring at IMO. Any data that is contractually protected as confidential by law or by contract and any other data that is considered by the Secretariat for confidential treatment should be regard as HS. HS data include, but not limited to:

.3.1 identity information about a delegate or staff member, (e.g. personnel records, biometric records, medical record, educational record, financial disclosure information) which if lost, compromised or disclosed without authorization could result in harm to that individual; and

.3.2 communication between a Member State and the Secretariat, which could expose the Organization or others to reputational damage or questions thereof, or other significant risk.

1.6 Category MS and HS data should only be collected or stored when it is for business and/or legal requirements. Aggregates of data should be classified based upon the most secure classification level. **When data of a mixed classification exist in the same document (e.g., file, report, etc.), the document should have the highest level of classification**. In the event that particular data has not been classified, as an interim control, it should be considered as either highly sensitive or moderately sensitive until it is properly classified.

1.7 The Director, Legal and External Relations Division, the Director, Administrative Division and ICT Services must be notified immediately if category HS data is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, as well as if any unauthorized use of information systems maintained by the Secretariat, has taken place or it is suspected that it is taking place.

Current data storage and information systems classification

1.8 A data classification exercise was embarked upon based on the system above. The result of the exercise has led to the assignment of similar data classification categories to the current data storage and information systems, which is based on the types of data they contain. It should be realized a data storage system is classified as HS if any data component contained therein is HS, irrespective of the use of such storage system or the volume of other data components that are not HS data. The outcome of the data storage system classification is set out in the annex, which will further assist staff members in classifying data they are working with, determining the appropriate environment in which to store such data and the level of access and exposure of such data should be given in the work place or externally.

2 DATA MANAGEMENT

Responsibilities

2.1 All stakeholders in the Secretariat have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the Organization irrespective of the medium on which the data resides and regardless of format (e.g., in electronic, paper or other physical form).

2.2 Each Division is responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission, and disposal of the Organization's data in compliance with the sensitivity as enumerated in this Policy.

2.3 The following roles and responsibilities should be considered in establishing a data management process:

.1 **Data Trustees/Owners:** Directors or their designees are Data Trustees/Owners within each Division. Data Trustee/Owner responsibilities include approving data access to staff, assigning data stewards, establishing divisional data protection procedures, and promoting data resource management for the good of the entire Organization.

.2 **Data Stewards:** Staff with direct operational level responsibility for information management. Data Stewards are responsible for working with Data Trustee/Owner to classify data, determining and specifying user access level(s), implementing and enforcing policy and procedures. This process is usually carried out during the design and implementation of new data storage and information systems and enhancements of existing ones.

.3 **Data Administrators:** Data Administrators are responsible for providing a secure infrastructure in support of the data including, but not limited to, providing physical security, backup and recovery processes, granting access privileges as authorized by data owners or their designees, and implementing and administering controls over the information.

.4 **Data Users:** Data Users are individuals who need and use the Organization's data as part of their assigned duties or in fulfilment of assigned roles or functions. Individuals who are given access to sensitive data have a position of trust, and as such, are responsible for protecting the security and integrity of the data.

2.4 Anyone who has intentionally breached the confidentiality and/or compromised the integrity of protected data/information (e.g., categories HS and MS data) may be subject to disciplinary action and/or further sanctions in line with Staff Rule 101.2(a) concerning "Staff member obligations and acts of misconduct".

2.5 Disposal of data: All MS and HS data in paper form should be shredded. Before data held on a computer system, electronic device or electronic media is disposed of, recycled or transferred, either as surplus property or to another user, the system, media or device must be properly sanitized of sensitive/confidential data and software, or properly destroyed. ICT Services should be engaged as appropriate on these issues.

***

Annex

Existing data storage and information systems and their classification based on the types of data contained therein

Data storage systems	Data Item	Where Held	Data classification
IMO email	(Entire system)	IMO Secretariat	HS
SAP system	(Entire System)	Logica-CGI*	HS
IMO file system	(Entire System)	IMO Secretariat	HS
	IMO Member memos/official letters/communications/ medical records		HS
	Secretariat administrative documents		MS
	H: drive, I: drive; J: drive; L: drive; M: drive; O: drive		MS
Secretariat Intranet (IMO@Home)	Entire system including e-forms, Correspondence logs etc.	IMO Secretariat	HS
	Correspondences log		HS
	e-Forms		MS
	e-Docs (Meeting document preparation)		MS
	OSG/Divisional Private data		MS
Registry Logs	All sectional registry logs (to be replaced by Correspondence log)	IMO Secretariat	HS
GISIS	Secretariat data	Secretariat/UNICC**	HS
	Member data		MS
	Validated public data		NS
	LRIT – data distribution plan		HS
IMODOCS	Working documents	IMO Secretariat	MS
	Finalized documents		MS
	Audio and video recordings		MS
	Circulars, Circular letters, Note Verbale etc.		NS
Public Website	www.imo.org	Secretariat	NS
	Facebook, Twitter, Blog, Tumblr, Flickr, Youtube	Cloud	NS

*Logica-CGI host SAP at their Data Centre. Contract with the Secretariat emphasizes the sensitivity of data and the need to protect it from unauthorized access.

** GISIS and LRIT-DDP is hosted at IMO Secretariat with a hot-standby copy of the system at UNICC Data Centre in Geneva. The facility allows for business continuity within a four-hour window when GISIS-LRIT in London is unavailable.

INTERNATIONAL MARITIME ORGANIZATION

IMO

E

COUNCIL
101st session
Agenda item 4

C 101/4/1
2 September 2008
Original: ENGLISH

ORGANIZATIONAL REFORMS

Public access to IMO documents on the IMODOCS website

Note by the Secretary-General

SUMMARY	
Executive summary:	This document makes proposals for providing public access to certain IMO documents on the IMODOCS website via the IMO public website
Strategic direction:	12.3
High-level action:	12.3.1
Planned output:	Not applicable
Action to be taken:	Paragraph 9
Related documents:	C 74/16, C 74/16/Add.1; C/ES.22/D; C 100/4(a)/1 and C 100/D

Background

1 The Council will recall the inception, as a pilot scheme in February 1995, of the Bulletin Board System (BBS), generously offered by the Government of Canada, through which Member States and organizations could access electronic versions of IMO documents. With the financial and technical support of Australia, Canada, Sweden, the United Kingdom and the United States, the BBS system was replaced by the IMODOCS system in 1998. IMODOCS was further enhanced in 2001 (Circular letter No.2300) and again in March 2008 (Circular letter No.2855).

Access to documents

2 At the outset, it had been decided that, during the first phase, the BBS would contain all pre-session documents of forthcoming sessions of meetings as well as notes verbales, circular letters and circulars. Other documentation (relating to reports and working papers) was to be added to the database at a later stage. In the first few months since the introduction of the BBS, only a limited number of Member States made use of the system. By the time of the introduction of IMODOCS in 1998, all meeting documents, including reports, were available through the IMODOCS website and its use by Member States, UN and Specialized Agencies, IGOs and NGOs has, since, increased significantly.

3 Subsequently, the Council, at its twenty-second extraordinary session in November 2003 (C/ES.22/D), further agreed that all the working papers approved by the sub-committees in plenary should be posted on the IMODOCS website.

4 The new expanded system went live on 4 March 2008. The transitional period of migrating user names and passwords previously used with the old IMODOCS ended in June 2008 following the issuance of Circular letter No.2892.

Public access to IMO information

5 The Council will further recall discussions at the 25th session of the Assembly and at its own 100th session (document C 100/4(a)/1) on the subject of making IMO documents publicly available. Some delegations, being in favour of increased transparency, advocated making all documents available, whereas others preferred to limit availability to prevent documents submitted to a session and not yet discussed being misinterpreted and/or misused.

6 Whilst endorsing the proposals contained in document C 100/4(a)/1, the Council requested the Secretariat to provide, for consideration at this session, a further analysis of the implications of making IMO meeting documents publicly available prior to the conclusion of the meeting in the context of which they were issued. This document aims at responding to this request.

7 In considering the timing of the release of IMO meeting documents on the IMO public website, a number of factors have been considered and a balanced approach sought with a view to ensuring that any information that is made available supports the IMO aim of access to information and transparency, whilst also ensuring, as far as practicable, that the proper conduct of IMO meetings is not compromised. On this basis, access to IMO meeting documents via the IMO public website is proposed in three categories, i.e. **prior to**, **during** and **post meetings**, as shown at annex. The simplified approach proposed aims not only to ensure a clear policy for the public availability of documents but also to facilitate clear guidance and instructions (electronically and operationally) for the Secretariat to comply with.

8 As a general policy, it is proposed that no public access would be allowed to any of the Council documents, including Council decisions and, in the event of a Committee deciding to hold all or part of any of its meetings in private, access to the relevant documents should also be restricted.

Action requested of the Council

9 The Council is invited to consider the proposed public access to IMO documents, as outlined at annex and decide as appropriate.

***

ANNEX

ACCESS TO IMO DOCUMENTS VIA THE IMO PUBLIC WEBSITE

DOCUMENTS	AVAILABLE
Prior to meetings	
- Agendas	Yes
- Session documents, i.e. submissions by the Secretariat, Member States and Organizations, including reports of correspondence groups and intersessional working groups	No
During meetings	
- Working papers	No
- Draft reports	No
Post meetings	
- Session documents*, i.e. submissions by the Secretariat, Member States and Organizations and correspondence groups	Yes
- Final reports of meetings*	Yes
- Assembly resolutions	Yes
- Final lists of documents	Yes
- Final lists of participants	Yes
- Council Documents and Decisions	No
- Summary Records	No

* Provided that there has been no decision to hold all or part of that particular session in private.