POWER AT SEA

NAVAL GROUP

BMS

BUSINESS MANAGEMENT SYSTEM

OPERATIONAL DOCUMENT: MARKING AND DATA PROTECTION MEMENTO INTENDED FOR SUPPLIERS

Version:	***EN***
Reference:	***000252741-B***
Process:	***HA - Purchasing***
Sub-Process:	***HA5 – Managing the execution of the contract***
Sub-sub-Process:	***N/A***
Activity or Activities:	***All***
Applicability:	***Naval Group***
Site(s):	***All***
Document status:	*Approved on* ***20/01/2023***

MARKING AND DATA PROTECTION MEMENTO INTENDED FOR SUPPLIERS

Delphine MOUCHEL

000252741-B / Approved on **20/01/2023**

Corporate Sensitivity
PUBLIC

DOCUMENT HISTORY SHEET

DOCUMENT APPROVAL CIRCUIT

APPROVAL		
Contributors	**First name Surname**	**Dates**
Written by	***Delphine MOUCHEL***	*N/A*
Checked by	***Valérie VITIELLO***	*N/A*
Approved by	***Gérard DUHAMEL***	***20/01/2023***

RECORD OF CHANGES

RECORD OF CHANGES		
Versions	**Description or reason for changes**	**Approval dates**
A	***First issue***	***14/12/2020***
B	***- Addition of the term "property" in the detailed legal notice on the first page of a document and for the following pages, in accordance with instruction BMS-110962*** ***- Clarification of French defence secrecy regulations*** ***- Addition of the Special France marking – third countries***	***20/01/2023***

YOUR COMMITMENT

You comply with the following 4 data management policies

Naval Group SA

1. INTELLECTUAL PROPERTY
4. CORPORATE PROPERTY (CP)

Regulatory framework

2. FRENCH DEFENCE SECRECY
3. EXPORT CONTROL (EC)

The markings presented are those that you will have to manage most frequently as part of your relationship with Naval Group.

You must also comply with the personal data protection clauses of the contract.

To ensure compliance with these rules, Naval Group will carry out verifications.

Any failure by the supplier to comply with this memento will result in a penalty of €1,500 per offence

DATA MANAGEMENT POLICIES AND THEIR MARKING(S)

1 INTELLECTUAL PROPERTY

Objective: specify the property rights of Naval Group SA after any Contract/Order.

Standard case: Naval Group SA owns the results stipulated in the Contract/Order

This marking is **mandatory** and must be written in English.

You must include the following on all deliverables:

- The Naval Group logo
- The copyright and legal notices

To be completed

Logo to be inserted at the top of the page:

NAVAL GROUP

Copyright and detailed legal notice at the bottom of the first page of a document (Word type):

© **Naval Group SA** property. All rights reserved "**year(s)**" (year of creation and year of the latest update). Both the content and the form of this document/software are the property of <name of the company> and/or of third party. It is formally prohibited to use, copy, modify, translate, disclose or perform all or part of this document/software without obtaining **Naval Group SA**'s prior written consent or authorization. Any such unauthorized use, copying, modification, translation, disclosure or performance by any means whatsoever shall constitute an infringement punishable by criminal or civil law and, more generally, a breach of **Naval Group SA**'s rights.

For the following pages:

© Naval Group SA property, "**year(s)**" (year of creation and year of the latest update), all rights reserved.

Copyright and detailed legal notice to be inserted into software, at the beginning of the file:

Copyright © **Naval Group SA** property "<MM[-YYYY]>", all rights reserved. Copyright © All rights reserved. Both the content and the form of this software are the property of **Naval Group SA** and/or of third party. It is formally prohibited to use, copy, modify, translate, disclose or perform all or part of this software without obtaining **Naval Group SA** 's prior written consent or authorization. Any such unauthorized use, copying, modification, translation, disclosure or performance by any means whatsoever shall constitute an infringement punishable by criminal or civil law and, more generally, a breach of **Naval Group SA**'s rights.

OUR DATA MANAGEMENT POLICIES and THEIR MARKING(S)

2 FRENCH DEFENCE SECRECY

For French suppliers

- The rules defined below are those resulting from the application of French regulations (IGI 1300). They take into account the laws in force in other countries pursuant to the security agreements established between France and other countries or specific security provisions.
- Classified information and media (*Informations ou Supports Classifiés* – ISC) such as documents, data, etc. are marked in accordance with the requirements of the regulations in force and the **Contractual security plans*** (*Plans Contractuels de Sécurité* - PCS).
- You must apply the French national regulations and general security agreements in force. For France, refer to General Interministerial Instruction No. 1300/SGDSN/PSE/PSD.

*** as of 1 July 2021, the Security Aspects Letter is replaced by the Contractual Security Plan (PCS).**

For foreign suppliers

- The marking must comply with the requirements of the **general security agreements (*Accords Généraux de Sécurité* - AGS) ,** or the specific provisions defined by the French Defence Procurement Agency (DGA) in the absence of any such agreements (specific agreements between **national security authorities**), or the specific security and **PCSI** provisions or **export licence** conditions, or in strict application of the **contract's security clauses**.

DATA MANAGEMENT POLICIES AND THEIR MARKING(S)

2 FRENCH DEFENCE SECRECY for French suppliers

Objective: Protect French Defence Secrecy (*Secret de Défense Nationale* – SDN)

DIFFUSION RESTREINTE

In France, information is protected as "Diffusion Restreinte" whenever the French State seeks to control its distribution and ensure its traceability when, for example (non-exhaustive list), this information:

- defines the choices made in the various spheres of national military activity or operational or technical security and which may be non-classified;
- constitutes a non-classified document or set of data whose dissemination must be limited and controlled in accordance with the provisions of a signed security agreement;
- could lead to the discovery of classified information by the concomitance of various “Restricted” information.

SPECIAL FRANCE

A document that is marked “Spécial France” may only be disclosed to a recipient of French nationality, located in France (or in an overseas French enclave) and working for a company governed by French law:

- The “Spécial France” marking is always placed alongside the “Diffusion Restreinte” marking (or a classification notice).
- The “Spécial France” marking may only concern certain parts of a document.

“Diffusion Restreinte” documents must be identified:

- on the first page with the references of the issuing body, the date of issue and the registration number;
- on each page, via the "Diffusion Restreinte" stamp placed in the middle of the page header;
- The "Spécial France" stamp is placed to the right of, or below, the "Diffusion Restreinte" stamp;
- For related documents, the "Diffusion Restreinte" stamp is placed in the middle of the cover page.

The font, size, line thickness and location are regulatory:

- Centred, Arial font, bold, size 18;
- Colour: red for "Diffusion Restreinte", blue for "Spécial France";
- Frame thickness: 2.5 points.

DATA MANAGEMENT POLICIES AND THEIR MARKING(S)

2 FRENCH DEFENCE SECRECY for foreign suppliers

Objective: Protect French Defence Secrecy (*Secret de Défense Nationale* – SDN)

DIFFUSION RESTREINTE

In France, information is protected as "Diffusion Restreinte" whenever the French State seeks to control its distribution and ensure its traceability when, for example (non-exhaustive list), this information:

- defines the choices made in the various spheres of national military activity or operational or technical security and which may be non-classified;
- constitutes a non-classified document or set of data whose dissemination must be limited and controlled in accordance with the provisions of a signed security agreement;
- could lead to the discovery of classified information;

SPECIAL FRANCE – third country

A document that is marked “Spécial France - Third Country” may only be disclosed to a recipient of the aforementioned nationalities located in one of the specified countries and working for a company governed by the law of the countries concerned.

- The “Spécial France – thierd country” marking is always placed alongside the “DIFFUSION RESTREINTE” marking (or a classification notice).
- The “Spécial France – Third Country” marking may only concern certain parts of a document annotated as such in the document's margins, however the document itself still bears the “Spécial France – Third Country” marking.

The country issuing a document with a level of sensitivity equivalent to the French “Diffusion Restreinte” marking must apply the equivalent marking provided for in the Protection Security Information (PSI) of the country concerned, validated by the national security authorities of the countries concerned.

“Diffusion Restreinte” documents must be identified:

- on the first page with the references of the issuing body, the date of issue and the registration number;
- on each page, via the Restricted stamp placed in the middle of the page header;
- The "Spécial France – third courntry" stamp is placed to the right of, or below, the “Diffusion Restreinte” stamp.
- For related documents, the “Diffusion Restreinte” stamp is affixed in the middle of the cover page.

The font, size, line thickness and location are regulatory:

- Centred, Arial font, bold, size 18
- Colour: red for "Diffusion Restreinte", blue for "Spécial France – Third country"
- Frame thickness: 2.5 points

RULES TO BE OBSERVED AND ENFORCED

FRENCH DEFENCE SECRECY MARKING for French and foreign suppliers

The rules apply to all operations performed using resources belonging to the supplier: premises, telephones, computers, information systems, printers, etc.

DIFFUSION RESTREINTE

SPECIAL FRANCE or **SPECIAL FRANCE – third country**

For all media and all actions (distribution, printing, storage, etc.) containing Diffusion Restreinte or Diffusion Restreinte Spécial France data, the supplier undertakes to:

- comply with and ensure compliance with the regulations (IGI 1300 and II 901 for French suppliers)*;
- obtain "Diffusion Restreinte" approval for its Information System (IS);
- ensure traceability of access to the information entrusted, and compliance with rules in terms of confidentiality and the need to know;
- alert the Contract Manager / Security Officer in the event of any incident.

**** II 901/SGDSN/ANSSI Interministerial Instruction of 28 January 2015 on the protection of sensitive information systems.***
http://www.sgdsn.gouv.fr/missions/proteger-le-secret-de-la-defense-nationale/

For all actions performed using a Naval Group resource, you must comply with the data protection memento - 000248984

DATA MANAGEMENT POLICIES AND THEIR MARKING(S)

3 EXPORT CONTROL (EC)

Objective: Identify whether the supplied Goods[1] are subject to Export Control in order to:

- Allow Naval Group to request authorisation (export licences) from the French administration if necessary → The supplier **must mandatorily** attach an Export Classification Certificate (ECC) to the Naval Group Orders or Contract.
- Comply with the licences granted by a foreign administration (End-User Certificate) → The supplier must ensure compliance with the regulations in force in their country or those inherited from their subcontractors (incorporation of foreign equipment).
- Ensure that Naval Group Goods[1] are not exported without authorisation from the French authorities → The supplier undertakes not to transmit the Goods[1] received from Naval Group to foreign subcontractors or foreign subsidiaries **without a licence**.

NOTE

In the case of Goods[1] subject to US regulations (ITAR[2] / EAR[3]), your responsibility is all the more important. These must be marked to ensure proper traceability, isolation, archiving and destruction.

[1] ***Goods subject to Export Control:*** *sensitive goods, services, software, technologies, sensitive data or information considered as War Material or Similar Materials or Dual-Use Items (civil and military).*
[2] ***ITAR****: International Traffic in Arms Regulations*
[3] ***EAR****: Export Administration Regulations*

RULES TO BE OBSERVED AND ENFORCED
EXPORT CONTROL MARKING

To be completed

POSSIBLE MARKINGS

Naval Group marking to the right of the Corporate Sensitivity stamp (as defined in the following slide)

<NATIONALITY>
EXPORT CONTROL

For a document issued on French territory

FRENCH
EXPORT CONTROL

ITAR marking in the footer on all pages

Warning: ITAR controlled

EAR marking in the footer on all pages

Warning: EAR controlled

In this case, the markings inform the supplier that the data is subject to export control in order to reinforce the prevention of any export or transfer without authorisation.

NOTE

Even if these markings are not mandatory, their absence does not allow goods to be transferred or exported to foreign third parties without Naval Group's explicit agreement and without obtaining a licence.

DATA MANAGEMENT POLICIES AND THEIR MARKING(S)

4 CORPORATE PROPERTY (CP)

Objective: Maintain control of Naval Group's industrial and commercial secrecy.

Corporate Sensitivity
PUBLIC

The information can be widely communicated to third parties. It involves general data about Naval Group. For example, the eco-design form.

Corporate Sensitivity
INTERNAL

The information cannot be distributed to third parties without a **legal connection** between Naval Group and the latter.

Corporate Sensitivity
CONFIDENTIAL

The information is **sensitive** and its disclosure to third parties in an unauthorised or uncontrolled manner could result in prejudice for Naval Group.

This information may only be communicated to persons with a **need to know** in the scope of a formalised legal relationship.

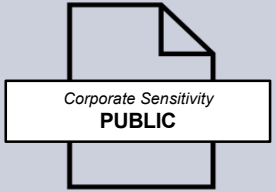
The need to know responds to the imperative need to become aware of information in the context of a specific function and for the proper performance of a specific mission.

Caution: this marking should only be used at the request of Naval Group.

Specific case of FORMS

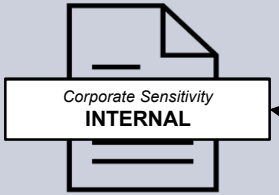
Case 1:
Standard form downloaded via the website or received by email

BLANK STANDARD FORM



A change of marking is required

COMPLETED FORM



Once the form has been completed, the supplier inserts the Corporate Sensitivity INTERNAL marking

Case 2:
Online form

FORM COMPLETED DIRECTLY ONLINE

No marking action to be performed by the supplier

RULES TO BE OBSERVED AND ENFORCED

COMPORATE ASSETS MARKING

CASE 1: PHYSICAL DELIVERABLES AND REMOVABLE MEDIA

AUTHORISED CONDITIONAL

BMS

The rules apply to any operation carried out using **resources that belong to the supplier** (premises, telephones, computers, information systems, printers, etc.).

ACTIONS / MARKINGS	SEND by post	STORE	DESTROY a physical deliverable	PHOTOCOPY	SCAN
Corporate Sensitivity **INTERNAL**	**AUTHORISED**	Inside a locked cabinet in a company room	**AUTHORISED**	Reproduction limited to the department's needs only.	In a company room, to an internal email address or using controlled storage means, excluding removable media
Corporate Sensitivity **CONFIDENTIAL**	Sent by registered post or authorised carrier, in a double envelope. Only the internal envelope contains the recipient's name	Inside a locked cabinet in a company room with access control	Using a cross-cut shredder. Failing that, to be sent by registered post or authorised carrier to Naval Group SA	Reproduction limited to the department's needs only. In premises with sufficient security conditions and that prohibit access to these documents by unauthorised persons	Same as INTERNAL + Reproduction limited to the department's needs only. In premises with sufficient security conditions and that prohibit access to these documents by unauthorised persons + ensure that the recipient has the need to know

Actions performed on a Corporate Sensitivity CONFIDENTIAL deliverable must comply with the need to know principle and ensure traceable access to the information entrusted in compliance with confidentiality rules.

The need to know responds to the imperative need to become aware of information in the context of a specific function and for the proper performance of a specific mission.

For all actions performed using a Naval Group resource, you must comply with the data protection memento – 000248984 (provided in the contract)

Corporate Sensitivity
PUBLIC

POWER AT SEA
RULES TO BE OBSERVED AND ENFORCED
COMPORATE ASSETS MARKING
CASE 2: DIGITAL DATA

AUTHORISED CONDITIONAL PROHIBITED **BMS**

The rules apply to any operation carried out using **resources that belong to the supplier** (premises, telephones, computers, information systems, printers, etc.).

ACTIONS / MARKINGS	SEND an email with an attachment	TRANSFER a large deliverable **(1)** to Naval Group / **(2)** to another recipient Prefer this method of transfer to email	COPY/STORE* a deliverable on an IT system	COPY/STORE* a deliverable on a removable medium	PRINT	DESTROY
Corporate Sensitivity **INTERNAL**	**Encryption of attachments required using the ZED or ACID tool**	(1) **Via a Naval Group exchange platform** (2) **Via a secure exchange platform**	**AUTHORISED**	**PROHIBITED** **prefer a secure exchange platform**	**Reproduction limited to the department's needs only. In a company room, from an internal email address or using controlled storage means, excluding removable media.**	**Destruction of the deliverable in a secure manner using the ACID tool or any other tool approved by National Agency for Security of Information Systems (*Agence Nationale de la Sécurité des Systèmes d'Information* – ANSSI)**
Corporate Sensitivity **CONFIDENTIAL**	**Encryption of attachments required using the ZED or ACID tools + Start the email subject with "CONFIDENTIAL"**	(1) **Via a Naval Group exchange platform by encrypting the deliverable using the ZED or ACID tool** (2) **Via a secure exchange platform by encrypting the deliverable using the ZED or ACID tool**	**Encryption of the deliverable required using the ZED or ACID tool + Prefix the name of the deliverable with "CS-CO"**		**Same as INTERNAL + In premises offering sufficient security conditions and that prohibit access to these documents by unauthorised persons**	

Actions performed on a Corporate Sensitivity CONFIDENTIAL deliverable must comply with the need to know principle and ensure traceable access to the information entrusted in compliance with confidentiality rules.

The need to know responds to the imperative need to become aware of information in the context of a specific function and for the proper performance of a specific mission.

For all actions performed towards Naval Group or using a Naval Group resource, you must comply with the data protection memento- 000248984

*** It is recommended to prefix files by their sensitivity level: CS-IN, CS-CO, DR, DRSF**

Corporate Sensitivity
PUBLIC

RULES TO BE OBSERVED AND ENFORCED

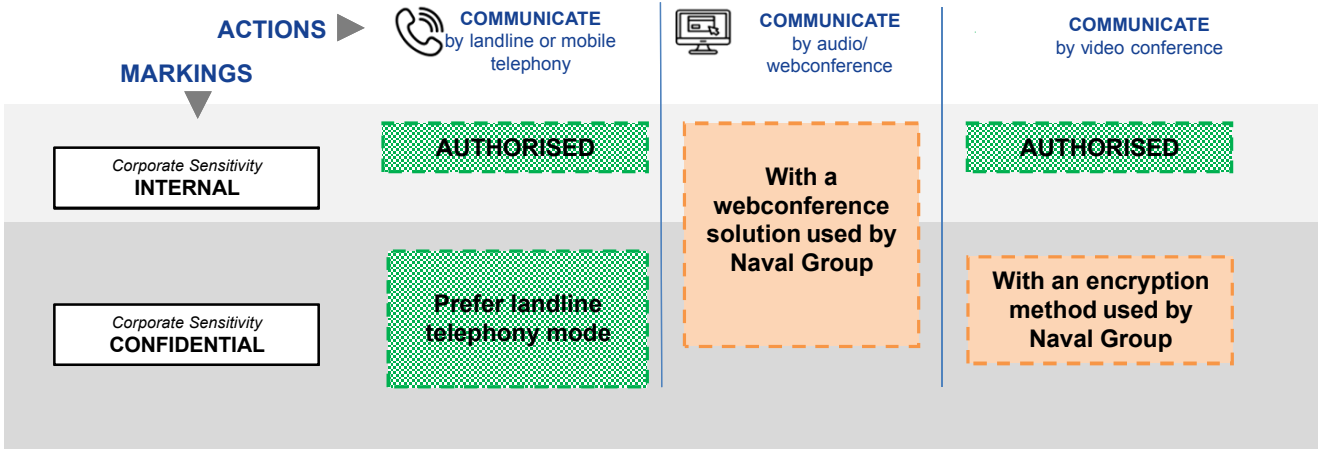
COMPORATE ASSETS MARKING

CASE 3: ORAL INFORMATION

AUTHORISED CONDITIONAL

BMS

The rules apply to any operation carried out using **resources that belong to the supplier** (premises, telephones, computers, information systems, printers, etc.).



Actions performed on a Corporate Sensitivity CONFIDENTIAL deliverable must comply with the need to know principle and ensure traceable access to the information entrusted in compliance with confidentiality rules.

The need to know responds to the imperative need to become aware of information in the context of a specific function and for the proper performance of a specific mission.

For all actions performed towards Naval Group or using a Naval Group resource, you must comply with the data protection memento - 000248984

Corporate Sensitivity
PUBLIC

TOOLS COMPLIANT WITH NAVAL GROUP REQUIREMENTS

BMS

**The tools below meet the Naval Group's data protection requirements.
Some of them may be imposed on you.**

Operation	Tools used by Naval Group*
TRANSFER large files within the group or outside the group	POSTFILES Reminder: this method is preferred over email transfer
COPY to external group resources (SAAS, cloud)	iExtranet
ENCRYPT/DECRYPT a file	ZED
ENCRYPT/DECRYPT and SIGN a file	ACID (Tool controlled by the French Defence Procurement Agency (DGA))
COMMUNICATE VIA AUDIO/WEBCONFERENCE	Orange Business Service Solution
COMMUNICATE VIA VIDEO CONFERENCE	TIXEO
COMMUNICATE VIA INSTANT MESSAGING	Citadel Team (private lounge with end-to-end encryption) WhatsApp is prohibited

*List may change

We must control the use of our data

Information sensitivity	Postfiles	iExtranet	Orange Audio / Web conference	Citadel Team	Tixeo
Corporate Sensitivity **PUBLIC**	Yes	Yes	Yes	Yes	Yes
Corporate sensitivity **INTERNAL**	Yes	Yes	Yes	Yes	Yes
Corporate Sensitivity **CONFIDENTIAL**	Yes (Zed or ACID encrypted)	Yes (Zed or ACID encrypted)	Yes (with 4-digit PIN)	No	Yes
Diffusion Restreinte	Yes (Zed or ACID encrypted)	Yes (Zed or ACID encrypted)	No	No	No
Diffusion Restreinte Spécial France	Yes (Zed or ACID encrypted)	Yes (Zed or ACID encrypted)	No	No	No
File sharing allowed via the tool	Yes	Yes	No	No	No

TO BE RETAINED
MARKING / PROTECTION

- **All documents must be marked** regardless of their level of sensitivity. The default marking is INTERNAL.
- **The Intellectual Property marking is mandatory and in English.**
- **There is no retroactive effect on current contracts**
- **Any exchange of INTERNAL or CONFIDENTIAL data is only possible if there is a contractual relationship (contract or NDA) and in compliance with export control regulations for exchanges with countries outside France.**
- **Use of the exchange platforms proposed by Naval Group is to be preferred.**

YOUR CONTACTS

If in doubt, contact:

- The Naval Group contract technical monitoring manager (otherwise the Naval Group buyer)


NAVAL
GROUP