NON SENSITIVE

BUSINESS MANAGEMENT SYSTEM

Version: *Bilingual*

Process: *01 DE – Managing the company*

Sub-Process: *DE9 - Ensuring the security of information, information systems, personnel and infrastructures of the Group*

Sub-sub-Process: *DE9.4 Defining and implementing the protection of the Group's Information systems (EIS, IIS, etc.)*

Activity (or activities): *All*

Scope of application: *01 Naval Group*

Site(s): *00 Tous*

Document status: *Approuvé* 27/03/2018

01 Instruction: User charter for information systemsUser charter for information systemsUser charter for information systems

000121750 - D

Summary: This charter formalises the rules applying to the use of Naval Group's Information Systems. It therefore ensures the security and performance of the system, the confidentiality of the data to be preserved in compliance with the applicable laws and the rights and freedoms recognised by Users. It establishes the rights and obligations of Naval Group, Administrators and Users of Information Systems and gives details of the checks performed on how they use these tools.

DOCUMENT HISTORY SHEET

APPROVAL		
Contributors	**First name Second name**	**Dates**
Written by		*25/01/2018*
Checked by		*26/03/2018* *27/03/2018*
Approval		*27/03/201826/03/2018*

BMS template used: BMS Instruction template, Guide, Organisation Document, Technical or operating document – Word format
000241821-C / Approved on 30/01/2018 / QP1.2 - QP8 / Naval Group / Site(s: All

		8

History of modifications		
Issue	**Description or reason for modifications**	**Approval date**
B	*First issue*	*04/08/2016*
C	*Integration of changes:* • *to the European rules concerning the protection of private data (General Data Protection Regulation, GDPR);* • *to the use of information systems (smartphone, social media, etc.).*	*30/01/2018*
D	*Document translation* *Approval circuit defined by note reference 18DQSE/0009 of 26/01/2018*	*27/03/2018*

CONTENTS

1 INTRODUCTION

1.1 PRECONDITION

Naval Group has information system tools that are essential to its activity. They are available for Users so that they can carry out their professional activities within Naval Group.

Their use must comply with the applicable legal and regulatory provisions and with the rules intended to protect information that is part of the intangible assets (including classified data) of Naval Group, and not to hinder the performance of processing implemented.

As such, the laws and regulations protect the rights of third parties and the rights of Naval Group, concerning notably intellectual property, personal data, trade secrets, information systems and they restrict freedom of expression.

In view of its activity, Naval Group has sensitive information that must be protected.

New methods of electronic communication involve risks inherent in the technology employed, both for Naval Group and for the Users. These risks may, notably, be caused by:

- uncontrolled disclosure of information;
- the possibility of obtaining access to protected or illegal information;
- the alteration or uncontrolled destruction of information of which the integrity and preservation are essential;
- the ease in which one becomes the perpetrator of violations or to be held liable.

The response to these risks involves technical means, the correct use of communication means and the vigilance of all those involved.

This Charter, hereafter named as "Charter", formalises the rules applying to the use of Naval Group's Information Systems. It sets out the rules which ensure the security and performance of the system, the confidentiality of the data to be preserved in compliance with the applicable laws and the rights and freedom recognised by Users. It establishes the rights and obligations of Naval Group, Administrators and Users of Information Systems and gives details of the checks performed on how they use these tools.

This Charter falls within the scope of the duty of loyalty and confidentiality of the User as regards Naval Group and within the commitment by Naval Group to respect the private life of Users.

1.2 DEFINITION

In this Charter, the terms below have the following meaning, unless the context requires otherwise:

"Administrator": Person (Naval Group employee, subcontractor, supplier) in charge of performing, in all the components of Naval Group's Information Systems (on site, remotely or by outsourcing), all the administration operations such as:

- the installation, development, support, update of Information Systems and programming codes;
- the backup and recovery;
- parameter setting, management of access rights or validation circuit;
- generation and distribution of access rights and other security supervision procedures;
- supervision of the correction operation of Information Systems;
- advice and assistance to Users.

"Authentication": Process used to check the identity of a user or a system before authorising access to resources and information of said system. The authentication of a user by an application is often done with a confidential code.

"Security needs":

- **Confidentiality**: ensures that only authorised people have access to resources which are exchanged and/or available;
- **Integrity**: ensures that the data, processing and systems are not corrupted throughout the production line of the services;
- **Availability**: ensures correct operation of the information system;
- **Traceability**: ensures that the actions carried out are preserved so that proof can be provided of their performance and accountability.

"Need to know" the need to only access the information which is useful and required for the User to perform their mission.

"Confidential code": sequence of letters, numbers and symbols allowing a user to sign in to a service or an application.

"User Account": identity and all access rights attributed to a user of a computer system.

"Encryption/decryption": operation in which a plain text is substituted for an unintelligible text which cannot be used by anybody who does not have the key which returns it to its initial state and vice versa.

"Management": People who have been granted signing authority or delegation of it from Naval Group's legal representatives.

"Personal data": Any information relating to a natural person who is or can be identified (hereafter referred to as the "concerned person"); is deemed to be a "natural person who can be identified", directly or indirectly, notably by referring to an identifier, such as a name, an identification number, bank details, location data, an on-line identifier or to one or several factors specific to his/her physical, physiological, genetic, psychic, economic, cultural or social identity.

"E-reputation": Reputation, general consensus (information, opinion, exchanges, comments, rumours, etc.) on the Internet concerning an entity (brand), legal entity (company) or natural person (individual), real (represented by a name or a pseudonym) or imaginary. It corresponds to the identity of this brand or of this person associated with the perception that Internet users have.

"Identification": Procedure used to safely identify a User or an Administrator.

"Information": For Naval Group, this designates files, databases, images, sounds, texts, videos, flow and all written or oral data, which is computerised or not.

"Nomad equipment" or "Removable equipment":Technical means, such as laptop computers, mobile phones, smartphones, tablets, terminals and peripheral devices (external or removable hard drive, magnetic medium, optical medium, USB key, PDA, network equipment, wireless equipment, remote communication board) used to obtain access to, transport or store data and which can be used outside Naval Group, whether connected or not.

"Social media": varied assembly of applications intended for the general public (social networks, blogs, wiki-websites, discussion forums, video or photo sharing, etc.), initially designed for personal use. These tools are used to create, exchange and widely circulate content generated by the Users themselves.

"Naval Group": Designates the Naval Group SA company which includes all the establishments, representative offices and branches.

"Security officer, information systems security officer": Person in charge of ensuring that Naval Group's activities in France are compliant with the legislative and regulatory framework of national defence secrecy, by participating in drafting security assurance plans, drafting security annexes and checking they are applied correctly, by assisting with site operations in analysing and controlling the security risk and by conducting actions to raise awareness and circulate information and to provide training for employees and service providers.

"Computer resources": Computer equipment (desktop or laptop computers, servers, removable equipment, nomad equipment, etc.), software, operating systems, telecommunication resources, as well as computing rooms. These resources can be accessed locally or remotely, directly or in series from the network belonging to Naval Group or on its behalf by a third-party.

"Telecommunication resources": All or part of Naval Group's telecommunication system, and in particular telecommunication terminals, such as routers, switches, encryption devices, telephone exchanges, faxes, printers, fixed and mobile telephones, smartphones, personnel digital assistants (PDA), tablets, IT networks and services such as Intranet, Internet, messaging systems, forums, instant messaging systems, social networks.

"Naval Group representative": Specifier for the supply of a product or service, responsible for requesting access to Naval Group's IS so that service providers can carry out their service.

"SaaS": *https://fr.wikipedia.org/wiki/Logiciel_en_tant_que_service*"Software as a service"; a commercial operating model which consists in jointly delivering means, services and expertise so that companies can completely outsource an aspect of their information system (messaging system, security, etc.), and to assimilate this as an operating cost (availability, operation) rather than an investment (acquisition cost, licences).

"Defence secrets": Information, processes, objects, documents, computerised data or files of interest to National Defence (and its international counterparts) which are subject to protection measures intended to restrict their circulation only to those authorised persons who "need to know".

"Industrial secrets": Information, processes, objects, documents, electronic data or files for which Naval Group, its customers and government organisations, define protection measures intended to restrict their circulation and in particular, trade secrets and the industrial and technical assets of Naval Group.

"Information security": All actions with an objective of integrity (the information is valid and has not undergone unauthorised modifications), confidentiality (only authorised people have access to the information exchanged), availability of resources and information processes (accessible within the specified time limits), authentication, (only authorised people have access to the information processes), traceability or the transaction is irrefutable, permanent availability of the information (archives are accessible, legible and integrated). Refer to security needs.

"Internet Services": The availability, through any means (local Intranet servers, local or remote modems, etc.) of various means of exchange and information, such as Internet services, external messaging systems, social networks, forums.

"Information systems": Naval Group's information processing and telecommunication system, including Industrial systems, which supply and distribute the information and allow, via IT and/or telecommunication resources, for it to be constructed, created, exchanged, circulated, duplicated, reproduced, stored and destroyed; an information system includes Internet services and social media.

The expression "information system" must be understood as grouping the information system itself, the processing information and the information processed by the system.

"Industrial systems": The industrial systems increasingly need to be connected to the Information System. They can take different forms, for example:

- Programmable Logic Controllers (programmable electronic system designed to automate industrial processes);
- Supervisory Control and Data Acquisition – SCADA (Industrial process control system which has a man-machine interface for supervision, and a digital communication network);
- Numerically controlled machine (Machine-tool which is numerically controlled);
- Test bench (Physical system used to put a product under configurable and controlled user conditions so that it can be observed and its behaviour measured);
- Sensors (Device used to detect a physical item (e.g.: light, heat, noise, electricity, etc.) and connected actuators;
- Ship Technical Management Systems (IT system used to supervise a range of information relating to ancillary systems – water, gas, electricity, air-conditioning, conditioning outside the so-called secure IS);
- Centralised Technical Management System (IT system used to process all the information from a specific sector: e.g. a technical installation such as an electrical power supply, heating/air-conditioning, lighting, etc.);
- Systems for site security (physical access control, intrusion detection and video-protection).

Belonging to Naval Group or made available by third-parties (the Government or the customer), these industrial systems include the following components:

- Field communication networks;
- Software and server, supervision and inspection station;
- Software and server, engineering and maintenance station;
- Analogue and digital sensors;
- Printed assemblies
-

"Processing personal data": Any operation or set of operations performed or otherwise using automated and applied processes for data or a range of personal data, such as obtaining, recording, organisation, structuring, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

"Users": Persons, linked by a contract with Naval Group or otherwise, of all levels, permanent or temporary, authorised to connect to Naval Group's information systems (i.e. with an account).

1.3 SCOPE

The obligations described in this Charter apply to any User/Administrator who has access to Naval Group's information systems, regardless of their access mode.

The Charter is an addition to the internal rules of each Naval Group entity in compliance with the French Labour Code. It completes the existing internal rules relating to the access and use of Naval Group's information systems and information.

The rules correspond to the management of specific secrets which are subject of an organisation and/or a specific regulation applying to this information and to these information systems, and this, notwithstanding the application of this Charter.

The use of IT and telecommunication resources by personnel representative bodies or for the exercise of a trade union mandate is the subject of a company agreement which is separate from the Charter.

This Charter is likely to make up a reference framework for the Group's subsidiaries in setting their own user rules but is imposed upon these subsidiaries when their IS is interconnected with Naval Group's IS.

1.4 OWNERSHIP OF INFORMATION SYSTEMS

The data presented in the information systems or conferred to a third-party (partners, suppliers, customers) is deemed to be of a professional nature and consequently, belong to Naval Group.

2 INFORMATION SYSTEM USER RULES

2.1 INFORMATION SYSTEM ACCESS POLICY

Naval Group defines the policy for accessing information systems and resources to which access must be protected.

Naval Group holds the rights and authorisations allowing each User to access the information systems. Any request for the allocation of access rights must be reasoned and formally validated by the authorised persons in accordance with the applicable procedures.

Naval Group reserves the right to grant, modify or refuse anybody the right to access its information systems.

The access and user authorisations granted to the User by Naval Group are strictly personal and confidential; the transmission or transfer, even temporary, to a third party is forbidden and assumes the responsibility of the persons concerned. Likewise, it is forbidden for any User to use the identifiers and passwords belonging to another User, unless otherwise specified in para. 2.2 below.

Each User must clearly identify himself/herself with the means supplied by Naval Group and must not use the identity of another person.

To this end, each authorised User has an individual and nominative access to the information systems and has an identifier and password to access the system.

This authorisation becomes invalid when the contractual association between Naval Group and the User is terminated, in the event that the Charter is breached, or in the event of a transfer. For security reasons, these access rights can also be suspended during an extended absence.

Any connection to the information systems, any transmission or use of data carried out by using the rights and authorisation of the User shall be presumed, unless proven otherwise by the User, to have been performed by the User.

A User is forbidden from using his/her access rights to access applications, information or an IT account other than those which have already been granted or for which he/she has received access authorisation.

2.2 MANAGING DEPARTURES AND ABSENCES

It is the User's responsibility, when he/she leaves permanently, to destroy his/her "private" directory and/or request a copy of his/her data from the Information Systems Department. Naval Group shall consider the content of the remaining files as professional data that can be used.

The "private" office directory of a User leaving Naval Group, if the User has not already destroyed it, will be deleted as soon as possible, unless there are legal proceedings and/or in the event of an act/action/fact which could lead to legal proceedings.

When leaving Naval Group, it is the User's responsibility to return all the IT means in good working order to the Department.

The departure of a User involves the immediate closure of his/her mail box, unless the Department decides otherwise. It is the User's responsibility to have his/her personal messages forwarded by giving his/her new address to the contact people concerned.

If the User is absent (leave or illness), Naval Group may have access, while respecting the User's privacy, to his/her to work data with the sole aim of ensuring that the activity continues.

To this end, the User accepts to communicate his/her identifiers and passwords to his/her line manager or to Naval Group's contractual representative.

In the absence of this communication, and in order to ensure the continuity of the activity, Naval Group reserves the right to take over or change the User's identifiers and passwords. The User concerned will be immediately informed of this operation by appropriate means as regards his/her situation and the new identifiers and passwords will be immediately communicated to him/her.

In particular, in the previously-mentioned cases, Naval Group can decrypt the files, if necessary.

In any case, if the User's work contract is suspended or terminated, the User is forbidden from using Naval Group's IT services.

3 RESPECT FOR THE LAW, REGULATIONS AND INTERNAL RULES

It is the User's responsibility to use any information system in compliance with the laws, regulations and usages, as well as this Charter, and to make sure that the interests of Naval Group are not harmed, nor those of others.

3.1 RESPECT FOR THE LAW AND REGULATIONS

This Charter is based on a group of legal and regulatory texts that all Users are deemed to be familiar with. It is notably the laws and regulations concerning:

- freedom of the press;
- protection of private data;
- respect for privacy;
- intellectual property;
- Naval Group's ethics code;
- protection of information systems;
- cryptology;
- the protection of national defence secrets.

The User who holds an authorisation which allows him/her to process defence secrets acknowledges having read the applicable instructions.

The personal responsibility of the User can be engaged for breaches, which can be qualified as criminal offences (infringement, insults, hacking, theft, sabotage, misconduct, negligence, etc.), that he/she commits or the damage that is caused.

The User must notably make sure that he/she:

- respects the intellectual property rights of authors and creators of software, texts, images, photos, videos, data bases;
- respects the property rights of Naval Group and the property rights of service providers. It should be noted that any unauthorised use of Naval Group's intellectual property rights shall constitute an infringement;
- prohibited information must never be collected or record in a computer memory, on paper or another format.

To this end, the following is strictly forbidden (the list is not exhaustive):

- to make copies of software (particularly freeware) for usage of any sort, copies of software can only be made by Naval Group's IT and Security department personnel, and this within the respect of the intellectual property rights of the software's author;
- to use the information systems for political or religious ends;
- to use the information systems to expose publicly or fully, an individual or collective request, except for the elected or designated personnel representatives, and this, within the framework and compliance with the applicable rules;
- to commit any action likely to call into question the physical or legal security of Naval Group, to adversely affect its reputation or to constitute any kind of prejudice;

- to adversely affect the information systems belonging to Naval Group or any other organisation;
- to transmit data retrieved from one of Naval Group's information systems to a third-party outside the scope of a contract;
- to commit any action implying or offending Naval Group's ethic reference system:
  - – concealment of identity by using pseudonyms (unless prior authorisation has been given by the Group's Security Department);
  - – any form of denigration and abusive or defamatory language with respect to Naval Group or its competitors or anyone else;
  - – games and/or dealings intended to obtain profit or personal gains (gambling activities, share market, etc.);
  - sexual and/or psychological harassment or sexist behaviour;
  - embezzlement of corporate funds, corruption, and any type of fraud;
  - and more generally, any illegal action, contrary to the Charter or to procedures applicable to Naval Group and any action likely to involve the civil and/or criminal liability of Naval Group.

3.2 RESPECT FOR INTERNAL RULES

The hierarchical, organisation and internal rules and internal authorities must be complied with.

The information handled and used is processed, recorded and exchanged exclusively on and using IT resources and telecommunication resources which have been authorised and parametered by Naval Group.

The information systems available to Users are for professional use within the exclusive limits of their functions.

The right of access is only granted to the User for use in compliance with his/her professional activity.

Any information processed by Naval Group's information systems is presumed to be of a professional nature.

In particular, the User must:

- read and strictly apply the reference system based on the Security Policy applicable to Naval Group as well as the procedures and their updates established by Naval Group, which are available and can easily be consulted at any time;
- ensure the protection and confidentiality of information which has been conferred to him/her; to this end, he/she is responsible for the rights that he/she gives to other Users and it his/her responsibility to protect the information by using different means such as backup or encryption which are made available in accordance with the sensitivity level of this information. He/she is in charge, at his/her level, of contributing to the general security;
- use suitable marking for the data according to the sensitivity level of the information and apply the corresponding protection measures in the interest of preserving Naval Group's tangible and intangible assets; (e.g. encryption of sensitive data sent by internal or external messaging system);
- use only the encryption tools in compliance with the internal procedures of Naval Group;

- signal any attempt to violate his/her account and, generally, any anomaly that can be determined which could be harmful to Naval Group or to another User;
- not use or try to use accounts which do not belong to him/her or to mask his or her genuine identity;
- not leave his/her work station, or another unattributed work station without disconnecting from the session in progress or locking his/her computer and he/she must not leave resources or services accessible to unauthorised people;
- not install, download or use on the IT equipment, any software or package without an appropriate user licence subscribed by Naval Group; not download new applications which have not been validated on the smartphone;
- not interfere with the smooth running of updates (antivirus, security patches, version upgrades) at his/her work station so that its vulnerabilities can be reduced; it is therefore strongly recommended that the User re-boots his/her work station each day instead of leaving it on standby;
- not modify the IT and telecommunication resources which have been conferred to him/her;
- not use personal IT resources for professional purposes (personal messaging system, removable discs, etc.) nor connect them to Naval Group's network.

He/she will keep in mind that the IT tool is shared and ensure that the user conditions are optimal for everyone, particularly in terms of storage capacity and network flow, by:

- limiting the size of downloaded files;
- only sending messages to addressees who are interested or concerned, to avoid saturating the network and servers, and thus not make the addressees read messages which do not concern them;
- not sending large numbers of messages;
- avoiding sending voluminous documents attached to the same message, by giving preference to compression tools or services dedicated to this usage;
- deleting messages sent and received which have become obsolete or are no longer useful;
- regularly archiving messages that have been received and sent.

Naval Group may require the User to use an electronic signature process to ensure the reliability and security of transactions relating to the access and to data.

The User is committed not to interfere, either voluntarily or by negligence, with the correct operation of information systems and communication networks and not to perform abnormal operations or introduce unsolicited software.

4 INTERNET SERVICES – ELECTRONIC MESSAGING SYSTEM

4.1 CONFIDENTIALITY RULES

In order the limit the risks of electronic messages being intercepted and to protect the interests of Naval Group, the use of the electronic messaging system for sensitive information must be limited to the strict minimum. This information shall be sent in compliance with Naval Group's applicable data protection policy.

The following information is considered to be sensitive (the list is not exhaustive):

- information about the customer and prospects;
- marketing strategies;
- embarked systems and products;
- contracts and partnerships;
- information about research and development projects, filing patents, etc.;
- unpublished financial data concerning Naval Group;
- information about employees and/or directors;
- architecture, systems, IT resources (data and programmes) and telecommunication;
- personal information, in particular telephone directories, flow charts (etc.);
- data and software developed internally by Naval Group or belonging to Naval Group.

Each User can only access information which is directly related to his/her function as well as his/her personal information or files.

The User is forbidden from trying to find out about information reserved for other Users.

Sending classified information through the conventional messaging system is forbidden.

Any data taken outside Naval Group must be recorded on encrypted or secured supports.

4.2 INTERNET SERVICE USER RULES

Because it is so easy to use, close attention must be given when writing and circulating electronic messages via the messaging system.

The electronic message is a written medium for which Naval Group can be held responsible.

No acknowledgement of responsibility, explicit or implicit, can be addressed by the User to a third party without having obtained express, prior authorisation from the Management.

The User must not modify the legal notices, confidentiality and non-responsibility clauses of Naval Group which are added when electronic messages are sent.

The User must be particularly careful not to open attachments or click on links sent with messages when the sender is unknown, the address appears to be false or when it concerns “spam”.

The Internet services must be used for professional purposes, in compliance with the Charter and the procedures applicable to Naval Group and in compliance with the applicable laws and regulations.

The following is forbidden (the list is not exhaustive):

- sending messages which are offensive, insulting, denigrating, defamatory, degrading or likely to adversely affect the privacy of people or their dignity, relating notably to race, national origin, morals, religion, political opinions, social origins, age, health, sex, gender identity or handicap, as well as messages adversely affecting the image, reputation or consideration of Naval Group (if such a message is received, the User must inform the Group Security Department who will prescribe the precautionary measures);

- consulting, copying or downloading the content of files or sites which refer to pornographic, paedophile, negationist, extremist or terrorist activity or are contrary to accepted standards or public order. These acts may be in the nature of a criminal offence which can be denounced to whoever it concerns, by the Management, without prejudice to the penalties of a disciplinary nature, such as specified in the internal regulations of Naval Group's sites;
- connecting to radio or television stations (except those associated with the function) or, downloading musical or film files, because of the congestion that they generate and the risk of breaching intellectual property;
- creating personal web pages;
- carrying out, with assistance from the information systems, work of any nature on his/her personal website;
- circulating the e-mail address on Internet sites which are not related to the professional activity;
- participating in electronic chain letters;
- using "CHAT" services, social networks, forums, blogs for personal purposes or to circulate sensitive information concerning Naval Group, its customers, suppliers or partners;
- transfer automatically or otherwise his/her professional messaging system to his/her personal messaging system, because this could jeopardise the confidentiality of Naval Group's sensitive data and compromise the accountability of sending messages to a clearly identified person;
- use Internet video services unless specifically authorised by Naval Group.

Furthermore, it should be noted that:

- no engagement, notably contractual, can be taken in the name of Naval Group by the intermediary of an Internet service without express, written authorisation in compliance with the rules applicable to Naval Group, notably in terms of delegating power and signature;
- any use of Internet services likely to commit Naval Group to a contractual relationship (engagement to pay, proposal of goods or services, etc.) must be subject of a prior, hierarchical authorisation;
- the User shall pay close attention to the fact that Naval Group is likely to be held responsible for certain exchanges with third parties by the intermediary of Internet services. This applies particularly to an abrupt termination of discussions which have been initiated;
- the User shall also take care not to accept on-line contracts by the use of a "click" or "double-click" without prior hierarchical authorisation.

4.3 USE OF SOCIAL MEDIA ON THE INTERNET

New risks for Users and Naval Group: identity theft, harm to image, circulation of sensitive information, lack of the right to be forgotten or even an approach from competitors, foreign intelligence services, participants with ill-intentions, etc.

Furthermore, communication through these types of media is considered to be in the public domain and is not protected by the confidentiality of correspondence.

Within the professional framework (on the premises and/or with the working tools), Naval Group's confidentiality regulations will prevail under all circumstances (refer to para. 4.4).

Outside work and using personal tools, the use of social media can have an impact on the security of people and information, intellectual property, the communication policy or the reputation of Naval Group.

Control of public profile

The User must control his/her public profile, particularly when it is be easy to find out that he/she works for Naval Group. The User must be aware that:

- information collected on various sites can be cross-checked to reveal a lot about him/her and the organisation of Naval Group and can be used to the detriment of the User;
- the identity of his/her contacts is not guaranteed;
- the circulation or ill-intentioned use of published information can be prejudicial, calling into question his/her professional credibility or making it vulnerable. Generally speaking, the User must not publish information that he/she may regret later when it is circulating in the public domain;
- the information published will be visible for a long time and the User will no longer control nor own this information;
- the content can become, without his/her knowing, widely accessible even if access is limited to people who are trusted;
- circulation of this information in real time means that the User can be located (geolocation) or too many details known about their schedule.

Furthermore, it is forbidden to:

- circulate confidential, sensitive or classified information (in any doubt, request advice, depending on the sector, from the Communication Department, Innovation and Technical Control Department or the security or information system security officer;
- indicate the clearances for National Defence secrets which are held by the User.

The User is held responsible for all his/her publications

The Communication Department is the only entity of the Group authorised to communicate in Naval Group's name on social media.

The User is forbidden from:

- communicating in Naval Group's name without authorisation. There must not be any ambiguity about the fact that the User is expressing himself/herself under his/her own name;
- using the name and graphic items which make up Naval Group's identity and image, without authorisation.

Copyright infringement is an offence, it is strongly recommended that the User:

- does not use content owned by Naval Group or when the origin of the ownership is not known or for which the User has not received assurance beforehand that he/she has the necessary rights to use and circulate this content (authorisation from the legitimate owner or content determined to have originated from the public domain);
- does not use personal data without assurance from the Data Protection Officer of compliance with the regulations relating to the protection of natural persons with respect to the treatment of personal data.

The company is a private location: recording, transferring without consent the image of a person is an invasion of privacy and any editing using the voice or image of a person without their consent can also be punishable as a criminal offence (art. L. 226-1 and art. L. 226-8 of the Criminal code).

Any video-surveillance system which aims to secure physical access to Naval Group's premises must comply with the applicable legislation concerning the protection of personal data.

Harm to "e-reputation"

In the event that, in spite of precautions, the User is subject to approaches from ill-intentioned participants relating to his/her professional activity, he/she must inform the security officer (or the information systems security officer) on his/her site and the Group Security Department.

The purpose of these instructions is to protect Naval Group and its employees from the risks which are inherent when using such media. They do not hinder the freedom of individual expression, or respect of private correspondence, guaranteed by the law.

4.4 PARTICIPATION IN FORUMS

Naval Group can be held responsible for the participation in forums. This participation is authorised exclusively for professional purposes and with the agreement of the User's hierarchy. In all cases, the User is not authorised to express himself/herself in the name of Naval Group without express, prior and special authorisation from the hierarchy.

With the exception of the instant messaging system supplied by Naval Group, it is also forbidden for any User to use direct interactive messaging software, such as "MSN Messenger" or "Yahoo Messenger" or "WhatsApp", etc..

5 SPECIFIC CASE OF REMOVABLE AND NOMAD EQUIPMENT

Any User who has nomad equipment (laptop computers, tablets or smartphones) or removable equipment made available by Naval Group is informed of the specific security instructions and the procedure to be followed in the event of damage, theft or loss of this equipment.

Only the authorised User can connect the removable and nomad equipment to Naval Group's networks. Only laptop computers, removable equipment (hard discs, USB keys, CD-Rom, DVD, memory boards, etc.), tablets and smartphones authorised by Naval Group can be connected to Naval Group's networks providing that these systems allow this connection.

The User's personal equipment cannot be connected to Naval Group's networks, or to those supplied by other companies (e.g. customers, partners, subcontractors, suppliers, school, etc.).

Removable storage supports containing personal data must not be used for professional activities, or be connected to Naval Group equipment.

The removable equipment, as soon as it is connected to an IT resource made available to Users by Naval Group to carry out their tasks, are assumed to be used for professional purposes; Naval Group can access files they hold which are not identified as personal, when the User is not present.

The content of professional removable storage supports must be encrypted by the tools made available at the workstation.

The User undertakes to check that this equipment is virus-free before introducing it to Naval Group's systems.

5.1 REMOVABLE AND NOMAD EQUIPMENT

The removable or nomad equipment is made available to the User in exchange for an acknowledgement of receipt.

When this equipment is used outside Naval Group, the User is responsible for looking after it when he/she is travelling (transport, hotels) and at his/her residence, with respect to their physical integrity and the confidentiality of data.

Before travelling abroad, the User must check that the systems he/she is taking only contain the information which is essential for the mission. Throughout the mission, the systems held must be continually monitored so that there is no physical contact with the equipment that the User may not be aware of. The User must not connect to Naval Group's network when he/she is located within a foreign government's area (ministry, military base, government agency, etc.), regardless of the mode of connection (wire, Wifi, GSM).

The use of removable or nomad equipment requires the User to exercise a reinforced level of surveillance and confidentiality. The Use must notably:

- scan the removable support on an antivirus terminal before any new connection to Naval Group's information system;
- make sure that a third party cannot take over the removable or nomad equipment, use it or access the content; otherwise, the User must immediately apply the above-mentioned instructions;
- Likewise, he/she must immediately notify the relevant departments of their loss, misappropriation or theft and the necessity to be able to supply the security organisation of the centre concerned with a copy of the record of information concerned by its disappearance.

The User must assist Naval Group or carry out himself/herself, depending on the case, all the initiatives (filing the complaint, declaring the loss or theft) required further to the incident, regardless of its nature.

5.2 SMARTPHONES/TABLETS

The professional smartphone is considered to be an extension of nomad-working (synchronising agendas, receiving professional e-mails, accessing Naval Group's information system, etc.). They are not intended to store data.

The User is forbidden from:

- using the camera function in military areas and in clearly identified zones within Naval Group;
- using a personal portable telephone within clearly identified zones where classified information and supports are exchanged;
- connecting the smartphone to workstations that have not been made available by Naval Group;
- installing new applications without express validation by Naval Group (the number of contaminated Android or iPhone Stores applications has increased significantly);
- receiving and storing sensitive data (Confidential, Restricted, For French eyes only) without any approved encryption installed and protection from encryption/decryption keys.

Personal use of a professional smartphone is tolerated providing this use is moderate. The Internet services must be used for professional practices in compliance with this Charter and Naval Group's procedures.

6 KNOWLEDGE MANAGEMENT AND ARCHIVING

Naval Group is committed to making a secured knowledge base system available to Users which will facilitate the work of capitalisation and knowledge sharing by integrating it in Naval Group's processes. The User is informed that he/she has limited storage space notably for the messaging system, shared directories and documentary spaces; to this end, each User must regularly sort and archive his/her information.

Naval Group is committed to maintaining the state of the art of the system by regularly making improvements and updates.

Users are informed of these regular improvements and updates.

Each User is committed to sharing his/her knowledge. To do this, the documents must be integrated in the knowledge management tools which are available, enriched and updated progressively as the work is performed.

Archiving

At his/her level, each User must make sure that archiving of information (paper, electronic) that he/she handles is carried out in compliance with the needs established by Naval Group and the legal and contractual obligations. This concerns:

- Any technical document which has an impact on Naval Group's know-how and which could be subject to feed-back;
- Any contractual document which has an impact on the customer and/or supplier relationship;
- Any administrative document which has a legal or statutory value;
- Any document which has a historical value so that Naval Group's history, trade and achievements can be better understood.

7 PRIVACY PROTECTION

7.1 PRIVATE USE

Use of Naval Group's information system for private purposes is tolerated given that it remains moderate, both in the frequency and duration, in compliance with the conditions and limits specified in this Charter.

In this context, it is the User's responsibility to store his/her private data (message, letters, etc.) in a data directory named "private".

All electronic exchanges which do not have the word "PRIVATE" (or "PERSONAL") in the subject are considered as professional exchanges. It is the sender's responsibility to judge whether a message is private. Each User must inform his/her contacts when his/her e-mail address is communicated privately.

The extra cost which could result (volume of data and volume of attachments which are exchanged) must remain negligible and this use must not have any adverse effect on the quality of work, nor the correct operation of the department and Naval Group, nor the time spent on working, in line with the correct operation of the information systems.

Its use must be rational in order to prevent saturation, destruction or misappropriation for personal purposes. It must comply with the applicable security policy.

Under the conditions of the articles of the Criminal Code guaranteeing the confidentiality of correspondence, Naval Group will not read the content of private messages, as well as private files on the message system, exclusively grouping the latter.

If there are specific and corresponding signs that the User has used the word “PRIVATE” (or “PERSONAL”) in an ill-intentioned or abusive way, Naval Group will have the right to take all the measures necessary on a disciplinary, and even legal level.

The abusive, private use will be deduced notably by the frequency of messages received or sent, of the volume of data exchanged, the format of attachments and the duration of connections.

7.2 PERSONAL DATA AND USER RIGHTS

In compliance with the applicable regulations relating to the protection of natural persons as regards the treatment of personal data, Users are informed that they have the right of access, rectification and opposition for a legitimate reason, relating to all personal information which concerns them, which is exercised by the Management.

8 INDUSTRIAL INFORMATION SYSTEMS

Naval Group's industrial systems increasingly need to be connected to Naval Group's network. In order to ensure the security of information systems, the User of the industrial system must:

- comply with the security policies and procedures relating to the industrial system;
- ensure compliance with protection measures against any environmental aggression or ill-intentioned act (sabotage, destruction) or negligence which could adversely affect the system's integrity;
- apply the physical and/or logical access checks which are attributed to him/her;
- only call on a third-party if they are qualified to work on the industrial system within the framework of its installation, maintenance or operation;
- report any attempt at intrusion or non-authorised act to the information systems Security Officer.

9 PROTECTION OF INFORMATION SYSTEMS

9.1 DATA BACK UP

Only professional data, stored in network directories, collaborative spaces, applications and professional messaging systems are systematically and periodically backed up. The backup frequency and duration that data is retained is defined by Naval Group according to the requirements and technical and organisational constraints.

The backup of local data located on the local hard drive of the work station, removable drives, USB keys and isolated work stations (outside the network) is the User's responsibility. The local archiving means can also be used for this purpose.

These means can be supplied by the Information Systems department. The Use cannot buy or use his/her own equipment to do this, under any circumstances.

9.2 INFORMATION SYSTEM ADMINISTRATION RULES

The Administrators manage the information systems (applications, servers, databases, workstations, networks, smartphones, tablets) placed under their responsibility in compliance with the administration tasks and the scope which has been conferred to them. They must ensure they are protected.

Access rights attributed to the Users must be consistent with the responsibilities (e.g. delegation limits) and tasks which have been conferred to them. They must comply with the following principles:

- need to know (access to sensitive information granted only to people who are authorised so that they can perform their function);
- separation of incompatible tasks which could cause errors or fraud (e.g. self-validation, etc.).

Access to privileged accounts is strictly limited and granted to Administrators according to a need and a specific usage, in compliance with a formal validation circuit, and this for a limited period of time, consistent with the responsibilities and tasks which have been conferred to them:

- separation of applicative administration and infrastructure administration tasks;
- separation of access rights management tasks from all other administration tasks;

- separation of development tasks from operating tasks;
- developers have access only to development and test environments,
- operators only have access to the production environment;
- project service providers and external auditors have temporary access to systems;
- …

Management of access rights to a collaborative documentary space is conferred to a manager who undertakes to regularly review and update the list of Users who are authorised to access this space due to their function.

Confidentiality

Further to the obligations which are imposed upon the Users, they are subject to the duty of confidentiality concerning personal or "private" data and any other sensitive data belonging to Naval Group to which they have access within the framework of their professional activities and even after the end of the contract which links them to Naval Group.

Availability

The Administrators are responsible for maintaining the quality of services supplied to the information system Users, within the limit of the means which are allocated to them.

To this end, they have the right to undertake any action necessary to maintain or re-establish the level of services in compliance with this Charter as well as Naval Group's security rules (anti-virus protection, installation of security patches, etc.).

Any software installed illicitly or any suspicious file shall be deleted as soon as its presence has been determined on the workstation, as well as on Naval Group's IT resources.

The Administrators have the duty to inform the Users as much as they can, of any palliative or corrective work likely to interfere or interrupt with the normal usage of the information systems.

Integrity of systems

The Administrators have the duty to immediately inform an information systems security officer from Naval Group and the Group Security Department of any intrusion attempt involving a system and any criminal behaviour of the Users or which does not comply with the Charter.

In the event of a contravention, the items gathered (serving as proof) shall be communicated to Management, according to the applicable security procedures.

Traceability

The trouble-shooting software as well as those for remote maintenance used by the Administrators to take remote control of the servers and work stations has the functionalities necessary for the transparency, traceability and confidentiality of data. Only software identified and kept up-to-date by the ISD after a decision by the GSD are authorised.

The use of this software made available to the Administrators is strictly limited to the needs of administration and trouble-shooting tasks.

For any remote work on the work stations, the Administrators must obtain prior agreement from the concerned Users.

These administration and troubleshooting activities are performed with respect for the privacy of Users; in compliance with the applicable legislation and in particular, the French data protection act.

9.3 CHECKING COMPLIANCE WITH THE CHARTER

Naval Group must carry out checks to make sure that the Charter is complied with.

Systematic checks or checks by sampling or according to elements which indicate a non-standard use may be performed by Naval Group on all the information systems made available to the User, at any time. These checks are performed so that all protection acts on the above-mentioned system can be carried out, in particular to protect against a non-compliant use that could harm Naval Group.

For legal compliance, protection against IT attacks, maintenance and technical management reasons, and in particular, in order to optimise the resources, certain types of content which are often the origin of incidents can be checked (problems with disc space, network congestion, chain distribution, "cookies", etc.).

Data collected during these checks can be preserved for an appropriate duration after the checking operations in compliance with the legal and regulatory provisions.

In this context, Naval Group has implemented systems to filter access which record the connection data in a journaled file. This journal is used to diagnose the anomalies or detect the intrusion attempts and to trace back to the source or the origin of the sender by specifying the name.

The User is informed that these systems in force can lead Naval Group to delete messages or files or interrupt their transmission or even remove (temporarily or permanently) the equipment made available.

Checks can be carried out on the use of the messaging system. In particular, they can deal with:

- volumes/the number of messages exchanged;
- the size of messages;
- the format of the attachments (images, videos, executables, compressed files, etc.);
- the quantity of disc space used;
- an analysis of messages (selection of words referring to pornography, racism, etc.).

Checks on the use of Internet Services can notably deal with the duration of connection, volumes transferred, sites visited. An analysis of the content of the sites visited and access filters to certain sites are implemented: sites distributing data of a pornographic or paedophile nature, racist or inciting racial hatred or radicalisation, terrorism, revisionist or containing data judged to be offensive.

Naval Group is able to check its incoming and outgoing traffic.

All traces of the User's activity are held by the information systems (sites visited, time of visits, downloaded items, type of text, image, video or software).

This monitoring is organised and supervised by the Group Security Department.

In the event that a User does not comply with this Charter, the Group Security Department shall be obliged to inform the User's line supervisor who can suspend or remove access rights to the account while a decision is made on any action to be taken and any other Department in the event of an offence, infringement or non-compliance with the applicable legislation.

10 RESPONSIBILITIES

Naval Group is responsible for:

- making the information systems available;
- the technical control of the information systems;
- securing the information.

All Users are responsible for the use of information systems to which he/she has access. Also, he/she must contribute to the general security of Naval Group, information and to the security of information systems.

The use of information systems must comply with the laws and rules and to the rules set out in this Charter. It must also be rational and fair, the User must avoid saturation of resources or their diversion for his/her personal gain.

It should be noted that the User is the only person responsible for using the identification elements and the rights transmitted to him/her by Naval Group in compliance with the aforementioned provisions of this Charter.

11 SANCTIONS

In case of non-compliance with the rules and measures listed in this Charter, the User is personally liable for the faults attributable to him/her and may be exposed, in a manner which is appropriate and proportionate to the breach committed, to the disciplinary sanctions defined in the internal rules, in addition to the possible immediate removal of his/her usage rights.

In the event that the charter is breached by someone who does not work for Naval Group, the User who is duly authorised by Naval Group and his/her employer, Naval Group reserves the right to:

- ask the employer of the person concerned for his/her immediate replacement with a person with an equivalent skill level;
- break the contractual relationship between the employer and the person concerned;
- seek compensation for the damages suffered by the employer and the person concerned.

Any abuse by the Administrators of the rights and privileges given to them in their professional administration practice is the subject of sanctions.

12 EFFECTIVE DATE AND ADVERTISING THE CHARTER

The Charter is annexed to the Internal rules and its effective date shall be one month after the legal formalities have been completed. It will be subject to the advertising required by the applicable regulations.

Each new arrival will be informed of the Charter's existence.

The Charter, which is part of the Internal Rules, will be displayed in compliance with article R.122-12 of the Labour Code.