Additional Security Requirements for the Intellectual Services General Purchasing Terms and Conditions

*****

Contents

Section 1 - Introduction

This document ("Security Requirements") supplements the Intellectual Services General Purchasing Terms and Conditions dated July 31 2013 (the "General Terms and Conditions"). As such, it sets out the additional security requirements that the Contractor agrees to comply with, and have its personnel and authorized subcontractors comply with, under an Order governed by these General Terms and Conditions, so as to guarantee the availability, access control, confidentiality, and integrity of the relevant Information Systems, as well as the traceability of any actions performed on these Systems.

The Security Requirements covered by the General Terms and Conditions apply to all types of Service. The additional security requirements described in sections 4, 5 and 6 of this document apply according to the typology of the Services covered by the Order or the cohesive standalone work section:
- The specifications for each Order or cohesive standalone work section will state the values of the characteristics of the Services covered by the Order or cohesive standalone work section according to the typology defined in section 2 below.
- The Security Requirements applying to the Order and/or to each cohesive standalone work section will be defined prior to starting work on the Services according to the applicability matrix described in section 3 below.

All security requirements applying to any Order shall be given prior validation by the Buyer's Information Systems Security Department and Security Department. All exemptions from Security Requirements shall also be submitted to these same departments for their prior written approval.

In the event of multiple requirements with the same purpose, the requirement(s) that are most restrictive for the Contractor will apply.

In order to ensure compliance with the Security Requirements the Contractor agrees to:

- set up a process for monitoring the application of these requirements throughout the period of execution of the Services,
- accept the performance of audits under the conditions set out in section 7 below.

Security Requirement terms given with a capital letter will take the meaning given in the General Terms and Conditions.

Section 2 - Typology of Orders or cohesive standalone work sections

The Security Requirements that the Contractor shall both comply with itself and ensure that other parties comply with depend on the characteristics of the Services covered by the following Orders or cohesive standalone work sections:

- type of Service,
- Contractor's level of responsibility,
- type of means used,
- geographic location(s) of the Contractor for execution of the Services,
- connection or not to the Buyer's IT network,
- level of sensitivity of the Order or the cohesive standalone work section.

2.1. Type of SERVICE

An Order may cover the purchase of several categories of Service.
These categories are given below:

- integration of software packages and software,
- corrective maintenance (software or software package),
- preliminary design study and design of Information Systems,
- software development and upgrade maintenance (on software or software packages),
- deployment and industrialization of the Information System (valid for corrective and upgrade maintenance, and software developments),
- technical expertise.
- remote code execution, remote control
- request management (call centre)
- hardware management
- remote control of workstations
- management of accounts/access rights
- preparation of masters and work sections
- local support (installation /support /maintenance /retirement)
- system operation and administration

2.2. Contractor's level of responsibility

Either the Contractor or the Buyer may be responsible for project management of the Services.

The main security guidelines are defined by the Buyer, and then applied and implemented during execution of the Services by the responsible contractor. In all cases, the Contractor is required to apply the defined Security Requirements, and to ensure their application by other parties.

2.3. Type of means used

Security Requirements will differ depending on whether:

- the hardware and software used to execute the Services are owned by the Buyer or the Contractor,
- the Buyer or the Contractor is responsible for installing, operating and administering these means.
- The level of sensitivity for the data processed and / or Buyer network requires.

Note that cases where the Contractor assigns hardware and/or software to the Buyer under the Order will be considered as cases where said hardware and/or software is the property of the Contractor.

Important note: This paragraph does not cover any possible computer link to the Buyer's IT network. This case is dealt with in article 2.5. below.

2.4. CONTRACTOR'S geographic location(s)

The place(s) of execution of the Order or cohesive standalone work section determines whether or not certain Security Requirements are taken into account.

There are four possible types of location:

- Buyer's site (including the establishment of a legal entity in which the Buyer is directly or indirectly the majority shareholder),
- rooms dedicated to the Contractor at a Buyer's site,
- a site, not owned by the Buyer, located on national territory,
- a site, not owned by the Buyer, located outside national territory,

2.5. Connection to the BUYER'S IT network

For the Contractor, connecting to the Buyer's IT network means:

- applying the Buyer's Security Requirements (technical and organizational) during Service execution,
- complying with computer system security regulations defined by the Buyer, especially in terms of computer system architectures or system operation.

2.6. Level of sensitivity of the Order or the cohesive standalone work section

There are four levels of sensitivity:

- Level 0: public domain.
- Level 1: subject to standard rules on professional discretion,
- Level 2: circulation restricted solely to persons needing to be informed for execution of the Services, and depending on their role in said execution,
- Level 3: confidential, i.e. subject to specific security measures.

Section 3 - Security Requirement Applicability Matrix

The Security Requirements are referenced as follows, yy being a number between 01 and 99:

"ELE yy"	Security Requirements specific to the place of execution of the services
"EPP yy"	Security Requirements relating to physical protection
"ESI yy"	Security Requirements relating to information systems

The first table below shows the numbers of the Security Requirements for Information Systems, Physical Protection or the place of execution applicable to all types of Service:

Service characteristics	Value of the characteristic	Place of execution	Physical Protection	Information Systems
	CLAUSES:	**ELE**	**EPP**	**ESI**
Whatever they may be	Whatever they may be	01, 05, 06, 09	01, 02, 03, 04, 05	06, 08, 09, 13, 25, 28, **33** 45,46,47,48,49, 50, 51, 53, 55, 56 62, 63, 64, 65, 66, 68, 69, 70, 58

The matrix below shows the Security Requirements for Information Systems or place of execution that apply to the Services supplied by the Contractor according to the characteristics of the Service covered by the Order or work section:

Service characteristics	Value of the characteristic	Place of execution	Physical Protection	Information Systems
		ELE	**EPP**	**ESI**
Type of Service	Integration of Software packages and software			01, 02, 04, 10, 11, 12, 37
	Corrective maintenance (software and software packages)			02, 03, 04, 05, 11, 30, 31, 34, 37
	Preliminary design study and design of Information Systems			01, 04, 10, 11, 12, 37
	Software development and upgrade maintenance (on software and software packages)			01, 02, 04, 11, 12, 31, 34, 37
	Deployment and industrialization of the information system			02, 03, 05, 10, 11, 12, 31, 34, 37 59, 60
	Technical expertise			01, 02, 03, 04, 05, 10, 11, 12, 30, 31, 34, 35, 37 54, 59, 60, 61, 67

	Remote code execution, remote control			01, 02, 03, 05, 10, 11, 12, 34, 35, 36, 37 60, 67, 69
	Request management (call centre)			01, 02, 04, 05, 37
	Hardware management			01, 03, 10, 11, 12, 37

Service characteristics	Value of the characteristic	Place of execution	Physical Protection	Information Systems
		ELE	EPP	ESI
Type of service (cont'd)	Remote control of workstations			01, 02, 10, 11, 12, 35, 37 60, 61 67, 69
	Management of accounts/access rights			01, 10, 11, 12, 34, 35, 36, 37 52
	Preparation of masters and work sections			01, 02, 05, 10, 11, 12, 31, 34, 36, 37 54
	Local support (installation /support /maintenance / retirement)			01, 02, 03, 05, 10, 11, 12, 30, 35, 37 54, 59, 60, 61 67
	System operation and administration			01, 02, 03, 05, 10, 11, 12, 16, 17, 19, 24, 26, 27, 28, 30, 35, 37 52, 54, 59, 60, 61 67, 68, 69, 70
Contractor's level of responsibility	Project management performed by the Contractor			38, 39
	Project management performed by the Buyer			NA
Type of means used	Administered by the Buyer throughout the period of execution of the Services			10, 20, 21
	Administered by the Contractor throughout the period of execution of the Services, and owned by the Buyer or assigned to the Buyer on completion of the Services			17, 20, 21, 40, 44 52, 54, 59, 60, 61
	Administered by the Contractor and not assigned to the Buyer on completion of the Services			23, 24, 36, 41, 42, 52, 54,59, 60, 61

Geographic location(s) of Contractor for execution of the Services	Buyer's site	08		26
	Rooms dedicated to the Contractor at a Buyer's site	03, 08		25, 26, 27
	A site, not owned by the Buyer, located on national territory	02, 07		06, 22, 25, 26, 27, 28
	A site, not owned by the Buyer, located outside national territory	02, 07		06, 22, 25, 26, 27, 28

Service characteristics	**Value of the characteristic**	**Place of execution**	**Physical Protection**	**Information Systems**
		ELE	**EPP**	**ESI**
Connection or not to the Buyer's IT network	Not connected			
	Remote connection to the Buyer's network	04, 07		18, 43
	Connection to the local network at the Buyer's site	04, 07		17, 18, 43,
Level of sensitivity of the Services	Level 0			NA
	Level 1			16, 42
	Level 2			16, 19, 24, 29, 32, 35, 36, 41
	Level 3			07, 16, 18, 19, 24, 29, 32, 35, 36, 41

Section 4 - Requirements covering the place of execution of the Services

ELE 01:
In all cases, the place of execution of the Services together with any modification to said location are subject to prior written approval by the Buyer's Security Department.

ELE 02:
If the Services are performed at the sites of the Contractor and/or its authorized subcontractors under article 21.2 of the General Terms and Conditions, the room used shall have an access control system with access traceability, shall be protected against intrusions and shall be under surveillance or remote surveillance both during and outside working hours.

Accordingly, within 1 month prior to starting work on the Services, the Contractor shall provide the Buyer's Security Department with a detailed description of the security systems at the site(s) for validation, including in particular:

- A description of the place of execution of the Services specifying the protection and access control and traceability systems deployed, including warden services and remote monitoring.
- A description of the computer system infrastructures and associated security systems.

Any modification of the security systems deployed by the Contractor and likely to impact on the Buyer's Information System or data shall be subject to prior written approval by the Buyer's Security Department prior to its implementation.

If the Contractor has to exchange data relating to the Services between its various sites or workplaces, these exchanges shall be encrypted and the process deployed shall be submitted to the Buyer's Security Department for its prior approval.

Furthermore, the Contractor's premises and its computer system connections will be subject to a preliminary conformity inspection by the Buyer's Security Department.

ELE 03:
If the Buyer provides the Contractor with a dedicated room at one of its sites for the execution of the Services, the Contractor agrees, within 1 month prior to starting work on the Services, to supply a description of the security systems (procedures, access, authentication, etc.) applicable at this location, together with the list of means and procedures used to monitor these systems for validation by the Buyer's Security Department.
This dedicated room and its computer system connections will be subject to a preliminary conformity inspection by the Buyer's Security Department.

ELE 04:
If the execution of the Services requires the installation of a computer system link between the place of execution of the Services and the Buyer's network, this link may only be installed following formal validation by the Buyer's Security Department of:
- the characteristics of the link, technical in particular, and the identification of the chain of operators performing the link,
- the proposed interconnection architecture.
If the Contractor has teams working on several sites or in different rooms at a single site, it may have only one single computer system link to the Buyer's network.

ELE 05:
If a security failure is identified in the computer system infrastructure or architecture at the place of execution of the Services, the Buyer reserves the right to suspend execution of the Services immediately at the Contractor's cost and to demand that the Contractor makes the relevant computer system infrastructure or architecture conform as quickly as possible.

ELE 06:
In the event of Service execution at the Buyer's site, the participation of any person (including the experts referred to in article ELE 09 below) likely to access the Information, results and their related media in any form whatsoever, as well as the computer system used to execute the Services, is subject to the Contractor submitting a prior written declaration to the Buyer's Security Department at least 15 working days before starting work on the Services.
This declaration is to be accompanied by a photocopy of the person's ID, and shall include the contact details of said person's employer, as well as details on the type of their employment contract.
For Buyer sites subject to regulations, current legislation applies (see EPP 02 for French sites: ERR, PS1, PS2, PS3, ESDA)
Wherever the Services are performed, the Contractor will have its personnel and any other person involved in the execution of the Services sign (i) the usage practice and security charter covering the Buyer's information systems and (ii) a non-disclosure agreement, and then send a copy of the signed documents to the Buyer's Security Department. These three documents are referenced in annex 1 "applicable documents".
The procedure described in requirement ELE 06 also applies to any person designated by the Contractor to replace another person working on the Services.

ELE 07:
For each place of execution, the Contractor keeps and regularly updates a list of all the persons working on the Services at one of its sites and/or at the site of one of its subcontractors as authorized under article 21.2. of the General Terms and Conditions. It sends this list to the Buyer's Security Department on request.

ELE 08:
For Services performed at the Buyer's premises, the list of persons operating the Buyer's computer systems is regularly updated by the Buyer's Security Department. The Contractor agrees to notify the Buyer's Security Department within 2 working days whenever a person is no longer involved in the execution of the Services.
The Contractor shall demand that any person involved in the execution of the Services at one of the Buyer’s sites is refused access to all installations at said Buyer's site other than those directly relating to execution of the Service.

ELE 09:
If, for the execution of the Service, the Contractor calls on outside experts likely to intervene on an occasional basis, the list of these experts shall be validated by the Buyer's Security Department.

Section 5 – Physical Protection Security Requirements

5.1. CONFIDENTIALITY

EPP 01:
In application of article 18.11. of the General Terms and Conditions, the Contractor agrees to ensure the security of Information and Results and their related media, in any form whatsoever, by applying the Buyer's Security Department regulations, and in particular by taking every useful and necessary measure such as:
· Affixing a confidentiality notice, stating at least "Restricted to (name of the Buyer's company)", to all documents or confidential media provided by the Buyer that do not already carry such a statement;
· Holding in a secure area all confidential documents or media whose access is restricted solely to persons approved by the Buyer,
· Management processes covering documents and related media, from their reception up to their destruction or restitution, in accordance with the applicable regulations and the Buyer's security requirements.

EPP 02:
The Contractor shall comply with local security field regulations where the facility is located.

5.2. Subcontracting

EPP 03:
As part of the subcontractor authorization procedure provided for in article 21.2. of the General Terms and Conditions and for security purposes, the Contractor shall send the Buyer prior written notification of its reasons for using a subcontractor.
The Buyer reserves the right to refuse the subcontractor without having to give reasons, or to authorize it provided that the subcontractor agrees to comply with security clauses additional to those required of the Contractor.

5.3. Non-solicitation of personnel

EPP 04:
Unless it has received the Buyer's prior written approval, the Contractor agrees not to make any direct or indirect offer of employment, nor to employ, in any form whatsoever, any member of the Buyer's personnel.
This agreement will stand throughout the period of execution of the Services increased by a further period of 12 months.
Should the Contractor fail to comply with this agreement, it shall compensate the Buyer by paying it an indemnity equal to the total gross remuneration paid to the employee during the 6 months preceding their departure.

EPP 05:
The Contractor agrees to comply with the regulations governing the processing of personal data and to provide the Buyer with all the information required for the relevant legal declarations.
It also commits itself on behalf of its own employees and subcontractors and will provide the evidence at the Buyer's request.

Section 6 - Information System Security Requirements

6.1. Authentication – Management of access rights

ESI 01:
The system shall make it possible to delegate user authentication to a third-party directory or provide for setting up automatic propagation of passwords from this directory.
It shall also provide for delegating the management of user access rights to this third-party directory, as well as automating updating interfaces between the system and the directory.

6.2. Configuration management

ESI 02:
Software upgrades shall be managed under configuration. It shall be possible to downgrade to the previous version.

ESI 03:
The Contractor guarantees the Buyer the ability to return the products (hardware, software, etc.) that it is working on to their original status prior to starting work on the Services (backtracking).
Any exception shall be subject to explicit prior approval by the Buyer's Security Department.

6.3. Hardware and software environment

CONTRACTOR'S ACCESS RIGHTS

ESI 04:

Unless there is a deterministic constraint expressly approved by the Buyer, the Services will be carried out on a dedicated environment with no continuous access to the production platform.
If necessary, and according to operational constraints, temporary access may be granted to consult the production platform. This access may be granted solely by the Buyer or any other person mandated by the Buyer, and according to the conditions validated by the Buyer's Information Systems Security Department.

ESI 05:
The Contractor has no access to the updating of production data.
The Buyer's personnel is responsible for performing data recovery when the system is in operational status.

ESI 06:
If computer system resources necessary to executing the Service have to be installed at the Contractor's site, the Contractor agrees to implement the means and procedures that provide effective access control of these resources.
These means and procedures shall ensure effective individual and transparent traceability of all individuals who have accessed these resources.

ESI 07:
The Contractor agrees to implement strong authentication means for Services with level 3 sensitivity.
The components of these strong authentication means shall be conform with the current state of the art at the time of Service execution, and with Safran Group technical standards (see annex 1)

ESI 08:
Access to computer system resources used to perform the Services is assigned by name to each individual involved.
If, for the execution of the Service, the Contractor calls on experts likely to intervene on an emergency basis, these experts will, where necessary, use emergency accounts in accordance with the "Emergency Accounts Management Procedure" listed in annex 1.

ESI 09:
The means and procedures used for access authorization and authentication of personnel needing to access computer system resources used for the Services shall make it possible to restrict the roles and privileges of said personnel to the strict minimum needed to perform their mission.

ARCHITECTURE

ESI 10:
The Contractor is to comply with current standards and technologies according to good practices in terms of the architectures and developments of secure IT systems.

ESI 11:
The Contractor is to comply with the Buyer's choice of architecture and technologies as well as with current Safran Group technical standards (see annex 1).

ESI 12:
In application of article 3.3. of the General Terms and Conditions, the Contractor shall make proposals aimed at upgrading existing architectures in order to maintain, or even improve, the level of security of these architectures.
In any event, the upgrading of these architectures is subject to the Buyer's written approval.

ESI 13:
The Contractor shall comply with the Buyer's security principles and regulations such as described in the documents dealing with this domain (see annex 1).

ESI 14:
Not applicable.

ESI 15:
Not applicable.

ESI 16:
The Result supplied by the Contractor as part of its Service shall include a tracking system designed to fit the sensitivity level of the Services. Prior to supplying the complete system, the Contractor is to send the Buyer's Security Department a detailed description of the tracking system and its operation for validation.
Should the Buyer refuse the system, the Contractor will submit a new solution to the Buyer for its written validation.

CHOICE OF HARDWARE AND SOFTWARE

ESI 17:
The hardware and software used or supplied by the Contractor as part of the execution of the Services shall be conform with the Buyer's current hardware and software standards (see annex 1).

ESI 18:

Not applicable.

ESI 19:
The hardware and software used for the Services and installed on the Contractor's premises will be isolated from the Contractor's own network, with no connection to the outside other than those explicitly approved by the Buyer's Security Department.

INSTALLATION, ADMINISTRATION, OPERATION

ESI 20:
The installation, operation and administration of the means implemented for execution of the Services shall be conform with good practices and the usage and security regulations set out by the Buyer (see annex 1).
Any exception will be subject to prior written approval by the Buyer's Security Department.

ESI 21:
Not applicable.

ESI 22:
The Contractor agrees to keep all traces of access from the device access control to premises for a period of three (3) months.
The Buyer may access this information immediately on simple request.

ESI 23:
Throughout the period of the Services, servers and workstations shall be installed and administered according to the good practices covering data protection and anti-intrusion systems, and shall be conform with Safran Group security standards (see annex 1)

ESI 24:
For Services with level 2 and level 3 sensitivity, the security systems relating to operational and administrational means will be submitted to the Buyer's Security Department for its explicit approval prior to starting work on the Services.

ESI 25:
The Contractor agrees to keep all traces of access to IT resources, including access to applications for a period of six (6) months.
The Buyer may access this information immediately on simple request.

ESI 26:
The Contractor shall provide the Buyer's Security Department at its request (via email, regular mail, fax) with all traces (service items and administrator documents) relating to the Services on the various computer systems used.

ESI 27:
Prior to starting work on the Services, the Contractor shall define a system that makes it possible to track Information Systems, and shall submit this system to the Buyer's Security Department for validation.
It will also ensure its deployment.
The traceability of computer systems shall not include any gaps without prior formal approval by the Buyer's Security Department.

ESI 28:
All operations to transfer memory, hard disks, archive or backup media are recorded in an operations log giving:
- All the levels of sensitivity of the Services: who (issuer and recipient), what (detailed), number, date,
- Level 2 and 3 Service sensitivity: time, place of collection, place of filing, identity of the forwarding agent,
- Level 3 Service sensitivity: routing details, identity of the forwarding agent's personnel responsible for the transfer.

The Contractor will send the Buyer this log on request.

In addition to this requirement, the Contractor shall comply with all the Buyer's current security regulations.

SERVICE EXECUTION AT ONE OF THE BUYER'S SITES

ESI 29:
The communication means used shall make it possible to guarantee the confidentiality of any information exchanged.
Unless decided otherwise in writing by the Buyer's Security Department, the link between the Contractor and the Buyer and/or any exchange of sensitive information made under the Services via the Contractor's own links between its places of work execution, shall be encrypted.
The Contractor shall submit the encryption means to the Buyer's Security Department for approval or refusal. The supply of the necessary means, together with the costs relating to the installation and use of these encryption means will be charged to the Contractor.

5.4. Test policy

ESI 30:
The Contractor is to make systematic basic non-regression tests.

ESI 31:
The Contractor is to make systematic functional non-regression tests prior to starting production.

ESI 32:
The datasets provided to the Contractor contain blanked out data.
The Contractor acknowledges having been notified and assumes the related risks.

5.5. Deliverables

ESI 33:
Prior to starting work on the Service, the Contractor agrees to propose a Security Assurance Plan covering:
- current and/or proposed measures guaranteeing that the Services conform with the security requirements such as defined in this document and its annex 1,
- the implementation and follow-up plan for these measures together with the corresponding security milestones.

This dossier will be subject to validation by the Buyer's Security Department prior to starting work on the Services.

ESI 34:
The Contractor is required to provide a Deliverable corresponding to the "ISS" (Information Systems Security) checklist covering installation and operational use, i.e. the list of security instructions to be followed during installation and/or use of the product.
This Deliverable will also include the list of utility accounts used or generated by the Contractor.

ESI 35:
The Contractor is required to provide:
For Services with level 3 sensitivity, a Deliverable describing all the actions it has performed during execution of the Services (including the list of the Buyer's data or datasets to which it has had access),
For Services with level 1 or level 2 sensitivity, a work report, at the least, at a level of detail to be specified by the Buyer at the start of the Service.

ESI 36:
For Services with level 2 or level 3 sensitivity, and prior to setting up the platform and/or starting work on the Services, the Contractor shall provide the Buyer with a Deliverable describing the methods for installing, administering and using the products.
This Deliverable will be subject to formal approval by the Buyer's Security Department.

6.6. Methodology / Practices

ESI 37:
The Contractor shall comply with the recommendations issued in the document "Group Technical Standards" (see annex 1). The Contractor is required to provide advice and proposals in this domain in application of article 3.3. of the General Terms and Conditions.

ESI 38:
The Contractor shall integrate security milestones throughout the period of execution of the Services. At each of these milestones, the Contractor shall demonstrate that it is following the Buyer's Security Requirements as specified in the Order, the General Terms and Conditions, the terms set out in this document, and in accordance with the characteristics of the Services.

ESI 39:
In application of article 7.1. below, the Contractor will submit any modification likely to impact on the security of the Deliverable, the Information System or the Buyer's data to the Buyer's Security Department for formal validation prior to taking it into account.

ESI 40:
Before transferring any hardware or software from the Contractor to the Buyer, a security audit will be carried out on the relevant hardware or software in order to check their conformity with the Buyer's security regulations that apply with respect to the Services.

ESI 41:
On completion of the Services and with no prejudice to the provisions of article 18.6. of the General Terms and Conditions:
Hard disks with level 3 sensitivity used by the Contractor during execution of the Services will be physically destroyed or returned to the Buyer at the Buyer's request and under its stated conditions.
The reassignment of hardware is not authorized.
The Contractor agrees to perform at least a strong data erasure procedure on any hard disks with level 2 sensitivity that it uses, in compliance with a procedure validated by the Buyer's Security Department prior to starting work on the Services. The Contractor will then send the Buyer a signed and dated data erasure certificate.

The Contractor agrees to perform at least a basic data erasure procedure (i.e. 7 overwrites) on any hard disks with level 1 sensitivity that it uses, in compliance with a procedure validated by the Buyer's Security Department prior to starting work on the Services. The Contractor will then send the Buyer a signed and dated data erasure certificate.

In all cases, the media used by the Contractor to execute the Services concerning the storage, transfer and backing up of information will be physically destroyed or returned to the Buyer, at the Buyer's request and according to its stated conditions.
In the event of destruction, the Contractor agrees to send the Buyer a signed and dated certificate of media destruction that includes an identification of said medias.

ESI 42:
Not applicable

ESI 43:
The Contractor agrees to comply with the security strategies implemented on the workstations used or provided as part of the Services (timeout, antivirus, no double connections, etc.) as well as with Information System Security regulations (passwords, etc.).
Information System Security regulations (ISS) are Safran Group regulations supplemented, where necessary, by regulations specific to the Buyer (see annex 1). These ISS regulations are to be forwarded to the Contractor as part of the tender.

6.7. Skills transfer

ESI 44:
Any transfer of hardware or software from the Contractor to the Buyer will be accompanied by a formalized transfer of skills to the Buyer's teams or to teams commissioned by the Buyer in order to take over the administration and operation of this equipment.

ESI 45:
In addition to the general provisions of the Safran Group Information System Security Usage and Security Charter (see ELE 06), the Contractor agrees to apply Safran Group directives concerning system administration and, in particular, to apply the security regulations and rules of professional conduct governing Safran Group Information System Administrators, and to have those members of its staff involved in the execution of the Service sign the individual subscription form entitled "Agreement to comply with the security regulations and rules of professional conduct governing SAFRAN Group Information System Administrators".

ESI 46:
Administrator accounts shall be managed in accordance with the Safran Group security directive relating to the administration of IS (see annex 1).
In particular, system passwords for "Administrator" accounts shall comply with Safran management rules on Administrator passwords.
These provisions apply to all access accounts, individual or otherwise, having technical privileges on all or part of the Buyer's equipment and systems and that the Contractor may have to use or manage as part of the Service.

ESI 47:
The Contractor agrees to immediately deactivate, or have a third party deactivate, any access account used by its workers in the following cases: termination of the mission of a member of the Contractor’s personnel for any reason whatsoever; the compromising (or suspicion of the compromising) of the access account.

ESI 48:

In the absence of a special provision explicitly planned between the Contractor and the Buyer, the Contractor agrees not to assign any administration privileges on the Buyer's Systems without prior, formal validation by the Buyer's Security Department.

ESI 49:
The Contractor agrees to set up and regularly update a depository with the Buyer's Security Department for all the "Administrator" accounts under its management.

ESI 50:
The administration platform for the Buyer's systems shall be hosted on an isolated network, firewall-protected against external intrusions and shall have no link to third-party networks and/or the Internet without the prior explicit agreement of the Buyer's Security Department.

ESI 51:
The technical means (tools and procedures) used for operating and administrating the equipment shall comply with the relevant Safran Group security principles. This is especially the case for local or remote work interventions and for the execution of code on the Buyer's systems and equipment (see technical actions in annex 1).
In the absence of a relevant Safran Group security standard, the technical means proposed by the Contractor shall be subject to prior explicit validation by the Buyer's Security Department.

ESI 52:
The technical means and management procedures governing password management shall comply with the relevant Safran Group security principles, and in particular those relating to:
- User and Administrator password strategies
- Troubleshooting or automatic troubleshooting systems
(see annex 1)

ESI 53:
All information belonging to the Buyer and stored on mobile media used by the Contractor for the Services shall be encrypted using a means validated by the Buyer whenever this information is not in the public domain (level 0).

ESI 45:
Hardware maintenance and transfer operations are subject to Safran Group security regulations and the Buyer's security procedures. This applies to removing hardware from the Buyer's sites, hardware reuse or replacement, or to equipment retirement or destruction.

ESI 55:
The Contractor agrees to implement antivirus protection systems on any equipment under its administration in accordance with the Group's antivirus policy (see annex 1) and the directives supplied by the Buyer at the start of work on the Services.
It also agrees to notify the Buyer's Security Department of any virus attack and to participate in managing Safran Group virus attacks.

ESI 56:
As part of the Services, the Contractor agrees to only use software that has been previously approved by the Buyer's Security Department.

ESI 57:
Not applicable

ESI 58:
The Contractor is to implement the technical means for supervising and monitoring systems, for managing disk areas and planning data processing operations in order to ensure proper system operation and security, within the limits of the Services assigned to it.
The Contractor agrees to do the following as quickly as possible:
- Notify the Buyer's Security Department of any incident capable of impacting on the security of the Buyer's Information Systems.
- Carry out or participate in any actions likely to mitigate an incident or at least minimize the effects and outcomes.

ESI 59:
The Contractor is to implement the means required to guarantee service continuity and data availability in accordance with the Buyer's service expectations as well as with the relevant Safran Group security standards (see annex 1).

It agrees to do the following at least:
- Implement a data backup/restoration strategy that includes the launch, execution monitoring and data restoration tests,
- Design an architecture with a sufficient level of redundancy.
- Keep available reports on the execution of backups and data recovery tests as well as its procedures and management charts.
- Store backup media in a secure location, at a frequency to be agreed with the Buyer, outside of server rooms and preferably outside the systems' host site.

ESI 60:
The administration and operation of systems and equipment are subject to technical procedures corresponding to the Buyer's needs and conform with good practices and Safran Group security regulations (see annex 1).
In particular, this is the case for activities involving the monitoring of service operation, stopping and start-up, management of security patches, deployments of systems and change management, monitoring of capacities and performance, etc.

ESI 61:
In addition to the provisions provided for under ECI 34, the Contractor will implement the provisions (tools and procedures) required to guarantee the regular and cohesive application of security patches to the systems and equipment that it operates and/or administers.
The expected results and the methods for implementing these systems will be defined at the start of work on the Services and submitted to the Buyer's Security Department for validation.

ESI 62:
As part of the audits carried out by the Buyer's Internal Audits Department, the Contractor will have to provide the evidence required under auditing of the Buyer's Security Department.
The purpose of these audits and their performance procedures are defined when starting Service execution.

ESI 63:
The physical and environmental measures for the protection of systems and equipment shall be conform with the relevant good practices and with Safran Group security standards.

ESI 46:
The Contractor will set up a procedure for tracking the security activity together with a regular review of events logs in accordance with the Buyer's directives.

ESI 65:
The procedures for managing accounts and access rights to systems and equipment are formalized. They include a monthly review that shall cover the following at least:
- The accounts possessing administration privileges on the IS,
- Obsolete accounts, in accordance with the Safran Group's standard security definitions and regulations (see annex 1).
Procedures and review reports shall be sent to the Buyer's Security Department at its written request (email, mail, fax).

ESI 66:
The Contractor agrees to set up an organization that complies with the principle of separation of privileges in accordance with Safran Group security directives (see annex 1).

ESI 67:
The IT equipment and infrastructure components (servers, workstations, printers, routers, switches, etc.) are to be installed and configured by the Contractor in accordance with the relevant good practices and with Safran Group security directives and recommendations (see annex 1).

ESI 68:
The Contractor agrees to carry our regular intrusion audits on all the systems it operates or administers.
It also agrees to send the Buyer the audit reports, to propose corrective and progress action plans for validation by the Buyer's Security Department, as well as to carry out these action and progress plans following their validation.
The frequency and scope of these audits will be agreed with the Buyer when starting execution of the Service, and will be carried out at least once every 3 years as part of general Safran Group IS security audit campaigns.

ESI 69:
Any change in the systems and at least in the infrastructure components impacting on IS security and/or their availability shall require formal validation by the Buyer's Security Department. The change management procedures for these components will be defined with the Buyer's Security Department when starting execution of the Service.

ESI 70:
The Contractor agrees to set up a computer system backup plan (PSI) covering the systems it operates and administers in accordance with the requirements of the services and business continuity defined by the Buyer and also with standard Safran Group security regulations (see annex 1).
In particular, it also agrees to:

- Test and update this PSI once a year at least,
- Send the Buyer the reports on the execution of the tests and the related progress plans,
- Implement the necessary progress plans.

Section 7 - Security audits - Penalties

7.1. SECURITY AUDIT

7.1.1.
In application of article 3.8. of the General Terms and Conditions, the Buyer may carry out or commission security audits by any third party of its choice subject to its confidentiality commitments, at any time, before and during execution of the Order, with no need to provide any reasons. The designated intervening party may not be a company that is a direct competitor of the Contractor within its skills area except in certain exceptional cases involving extremely concentrated markets. The Buyer also agrees to have each expert missioned to carry out an audit sign an individual confidentiality commitment.

Audits may also be carried out:

- by the Buyer's supervisory authorities as part of their mission to audit the Buyer,
- as part of the Buyer's internal Audit process.

The Contractor agrees to work with any designated auditor in good faith and with no reservations. Accordingly, it will answer any questions and facilitate the auditors' access to any document or information or other item useful to the smooth running of the audit mission.

Moreover, in cases where the Contractor subcontracts part of the work entrusted to it by the Buyer, the Contractor agrees to carry out a security audit of its subcontractors at its own cost, and at least once a year. The purpose of this audit will be to check the conformity of subcontractor(s) operations with the Security Requirements set out in the General Terms and Conditions and in this document. On completion of the audit, the Contractor will send the Buyer's Security Department a copy of the audit report.
In the event of subcontracting at n levels, the Contractor agrees to ensure that each subcontractor, at any level whatsoever, may be audited accordingly.
The audit will be subject to a report that will remain confidential between the Buyer and the Contractor.

These audits will not, under any circumstances, release the Contractor from its obligation to comply with all its contractual requirements nor will they signify the Buyer's agreement to or ratification of any nonconformities with the Security Requirements attributed to the Contractor.

7.1.2.
These audits cover compliance with the security requirements applicable to the Services, including in particular:

- The safety of premises and personnel;
- The tools, means and procedures implemented by the Contractor for the execution of the Services, including the security means relating to the operation and administration of the systems where necessary;
- Technical and security choices, as well as validation of the resources used for the Services;
- The monitoring of physical and computerized traces relating to the execution of the Services;
- Accuracy of the reporting items, in particular concerning business volumes and service levels produced;
- compliance with the planned rules for maintaining the conditions of reversibility;
- The implemented security regulations;
- The vulnerability of the systems either belonging to or installed by the Contractor.

Accordingly, it has been agreed that the Contractor will not invoice any price supplement due to extra work induced by security audits, within the limit of a credit of 30 Man-Days per year and per Buyer. Beyond this credit amount, the Contractor will invoice the time spent by its staff based on the evidence and according to the tariffs agreed previously with the Buyer.

Should any audit report, whether commissioned by the Buyer or another party, reveal a breach of the Contractors' obligations, the latter shall implement and/or have its authorized subcontractors implement the relevant corrective measures within the time required by the Buyer, and according to the criticality of the breach (see table below in section 7.3), as from the time the Buyer is notified and at the Contractor's sole expense, with no prejudice to any penalties provided for in section 7.2. below.

7.2. Penalties

Any breach in the Security Requirements identified by the Buyer may result in unauthorized persons being refused access to the Buyer's sites or information systems; the Contractor would not, however, be able to use this access refusal as an excuse for evading the execution of all its obligations under the Order and, where applicable, would be exposed to legal proceedings, in particular in application of the applicable regulations governing the disclosure of information covered by Defense secrecy.

In the event of noncompliance with the provisions set out in the Security Requirements by the Contractor, its staff or its subcontractors, the Buyer also reserves the option of:

- Refusing to accept Order Deliverables for the purposes of security.
- Applying penalties to the Contractor,
- In application of the General Terms and Conditions, terminating the Order automatically with no advance notice by simple notification addressed to the Contractor, with no damages and interest payable to the Contractor due to the termination,
- Beginning legal proceedings where necessary. In particular, the Buyer reserves the right to begin legal proceedings before a criminal court against the Contractor's personnel and subcontractors who have used or attempted to use access to the Buyer's network for the fraudulent copying, unauthorized modification or destruction, or malicious use of data, software or software items belonging to the Buyer.

Each Security Requirement is related to one or more risks, which are qualified by a criticality level and one directive providing a solution to the risk(s).

The criticality level is defined by a value between 1 and 5. Value 5 corresponds to maximum criticality. Value 1 corresponds to minimum criticality.

There are two types of risk:
- risk impacting the Buyer's security level (used data, security regulations),
- risk impacting the security level of the product produced by the Contractor.

Risk impacting the Buyer's security level:
Each risk impacting the Buyer's security level will be linked to one of three possible deadlines for restoring compliance:
- immediate restoration of compliance (0 days)
- restoration of compliance within 5 days
- restoration of compliance within 10 days

Risk impacting the security level of the Results produced by the Contractor:
Each risk impacting the security level will be linked to a deadline for bringing into compliance.
This deadline for bringing into compliance will be proposed by the Contractor and submitted to the Buyer's Security Department for validation.

Principles for calculating penalties:

Penalties will be applied in the event of an anomaly capable of impacting the Buyer's security, as well as in the event of overrunning the deadlines for bringing into compliance such as defined in this section and/or at the start of work on the Services.

The amount of and method for calculating penalties will be defined prior to starting work on the Services and shall comply with the following principles:

- Grading of the penalty according to the level of criticality of the anomaly's impact
- Exponential and non-linear increase of the penalty according to the number of days of delay for bringing back into compliance
- Exponential and non-linear increase of the penalty in the event of the anomaly being repeated.

A status report on the security anomalies recorded during execution of the Services including, for each anomaly, a status report on the bringing into compliance and the related deadline is produced on a regular basis.
This status report is used to calculate the related penalties.

The payment of penalties by the Contractor does not release it from its obligation to comply with the Security Requirements, and does not prejudice the Buyer's rights to request compensation for the damage suffered due to the Contractor's breach of obligations.

The table below gives the classification used to establish the above-mentioned financial penalties. Classification of the risks linked to the requirements:

Reference of the requirement	Description of the risk (where several risks are linked to a given requirement)	Level of criticality	Bringing into compliance to a given deadline
ELE 01	Site not declared previously	5	0 days
ELE 02	Site modification performed without the Buyer's prior approval	5	0 days
ELE 02	File not supplied by the Contractor	4	0 days
ELE 02	The Contractor supplies an incomplete file or the Buyer refuses the proposed means	2	5 days
ELE 02	Nonconform premises	5	0 days
ELE 02	Nonconform connections	5	0 days
ELE 03	File not supplied by the Contractor	4	0 days
ELE 03	The Contractor supplies an incomplete file or the Buyer refuses the proposed means	2	5 days
ELE 03	Nonconform connections	5	0 days
ELE 04	Links not validated or refused by the Buyer and used by the Contractor	5	0 days
ELE 05	Proven shortcomings, without the Buyer's prior approval	5	0 days
ELE 06	The intervening party fails to sign the documents	1	0 days
ELE 06	The intervening party is not declared prior to starting work	4	0 days
ELE 06	Noncompliance with the IT charter	4	NA
ELE 06	Clear and repeated failure to take account of the Security Requirements by the Contractor or the person acting in its name	5	0 days
ELE 06	Noncompliance with the signature procedure	2	NA
ELE 07	Absence of a declaration on mission completion	4	0 days
ELE 07	No list or list incomplete	3	2 days
ELE 08	Absence of a declaration on mission completion	4	0 days
ELE 08	Failure to wear a badge	2	0 days
ELE 08	No list or list incomplete	3	2 days
ELE 09	Noncompliance with the emergency intervention procedure	3	0 days
EPP 01	Transmission to an unauthorized person	5	0 days
EPP 01	Failure to apply data protection measures	5	10 days
EPP 02	Noncompliance with the legal obligations	4	0 days
EPP 03	Unauthorised subcontracting	4	0 days
EPP 03	Subcontractor's noncompliance with the security regulations	5	10 days
EPP 04	Not applicable	NA	NA
ESI 01	No management of access rights outside the software package or non-automatic authentication propagation	2	Depending on the Service
ESI 02	No configuration management	3	Depending on the Service
ESI 02	Impossibility of downgrading to the previous version	4	Depending on

Reference of the requirement	Description of the risk (where several risks are linked to a given requirement)	Level of criticality	Bringing into compliance to a given deadline
			the Service
ESI 03	Impossible to downgrade to the previous version	4	Depending on the Service
ESI 04	Services performed on a non-dedicated environment	4	0 days
ESI 04	Access to the production platform: noncompliance with the regulations – modification / consultation in continuous access, compliance with local RSSI regulations	5	0 days
ESI 05	Contractor gains access to production data	5	0 days
ESI 05	Data recovered by external personnel	5	0 days
ESI 06	Access to data by a person whose identity cannot be found	2	NA
ESI 06	No traceability system or a traceability system resulting in ambiguities	3	5 days
ESI 06	Inexistent or ineffective control of access to resources	4	5 days
ESI 06	One ID matches several individuals	4	0 days
ESI 07	Authentication means set up by the Contractor do not meet the required level	5	0 days
ESI 08	Noncompliance with the emergency account procedure	1	0 days
ESI 09	Access privileges too broad in relation to the need	3	0 days
ESI 10	Noncompliance with secure technologies and standards	5	Depending on the Service
ESI 11	Noncompliance with the Buyer's choice of architecture and technologies	3	Depending on the Service
ESI 12	The Contractor does not submit proposals	2	Depending on the Service
ESI 13	Noncompliance with security guidelines	3	Depending on the Service
ESI 14	Insufficient level of redundancy	4	Depending on the Service
ESI 15	Not applicable	Not applicable	Not Applicable
ESI 16	Product non conform in terms of traceability	3	Depending on the Service
ESI 17	Non-standard hardware and/or software connected to the Buyer's local network or administered by the Buyer	4	0 days
ESI 17	Non-standard hardware and/or software NOT connected to the Buyer's local network and NOT administered by the Buyer	2	5 days
ESI 18	Non-standard hardware and software	4	5 days
ESI 18	Administration by the Contractor	5	0 days
ESI 19	Contractor's means not isolated	5	0 days
ESI 19	Detection of a non-approved external connection	5	0 days
ESI 20	Installation and procedures non conform with the state of the art	3	5 days
ESI 20	Installation and procedures non conform with the Buyer's regulations, and ESI 24 not applicable	5	0 days

Reference of the requirement	Description of the risk (where several risks are linked to a given requirement)	Level of criticality	Bringing into compliance to a given deadline
ESI 21	No planned upgrade scenario	3	Depending on the Service
ESI 22	No traces of conservation access for 3 months or no response to requests from the Buyer	4	5 days
ESI 23	Noncompliance with the state of the art	3	5 days
ESI 24	Noncompliance with the Buyer's requirements	5	Depending on the Service
ESI 24	No prior validation by the Buyer	3	Depending on the Service
ESI 25	Access records not kept for a 6-month period or no response to the Buyer's requests	4	5 days
ESI 26	No response to the Buyer's requests	4	0 days
ESI 27	No prior formal validation by the Buyer	5	Depending on the Service
ESI 27	Proven shortcomings, without the Buyer's prior approval	4	5 days
ESI 28	No log or log incomplete	5	0 days
ESI 28	Noncompliance with the Buyer's regulations	5	0 days
ESI 29	Links not encrypted	5	0 days
ESI 29	The Buyer has refused or failed to validate the setting up of an encryption system	4	0 days
ESI 30	No basic non-regression test	4	Depending on the Service
ESI 30	Basic non-regression tests incomplete	3	Depending on the Service
ESI 31	No functional non-regression test	4	Depending on the Service
ESI 31	Functional non-regression tests incomplete	3	Depending on the Service
ESI 32	NA	NA	NA
ESI 33	The Contractor has not submitted a compatibility study	4	Depending on the Service
ESI 33	Work started without the Buyer's validation	5	Depending on the Service
ESI 34	The Contractor has not supplied a deliverable or the deliverable has major shortcomings	5	Depending on the Service
ESI 34	Incomplete supply containing minor shortcomings	3	Depending on the Service
ESI 35	The Contractor has not supplied a deliverable	5	Depending on the Service
ESI 35	Deliverable containing major shortcomings	5	Depending on the Service
ESI 35	Incomplete supply containing minor shortcomings	3	Depending on the Service
ESI 36	The Contractor has not supplied a deliverable	4	Depending on the Service
ESI 36	Work started without the Buyer's validation	5	Depending on the Service
ESI 37	Noncompliance with the Buyer's standards with no prior authorization	5	Depending on the Service
ESI 37	The Contractor does not submit proposals	3	Depending on the Service
ESI 38	Service rollout does not include any security milestones	5	Depending on the Service

Reference of the requirement	Description of the risk (where several risks are linked to a given requirement)	Level of criticality	Bringing into compliance to a given deadline
ESI 38	Milestones are not correlated with the requirements	4	Depending on the Service
ESI 38	Noncompliance with Security regulations	5	Depending on the Service
ESI 39	The Contractor has not submitted a request	5	Depending on the Service
ESI 39	Work started without the Buyer's prior validation	5	Depending on the Service
ESI 40	No security audit has been carried out	4	Depending on the Service
ESI 40	Non conform hardware and software	2	Depending on the Service
ESI 41	Erasure performed but no certificate sent out	1	5 days
ESI 41	Erasure not performed	5	0 days
ESI 42	Erasure performed but no certificate sent out	1	5 days
ESI 42	Erasure not performed	4	0 days
ESI 43	Noncompliance with the Buyer's security regulations and strategies	5	0 days
ESI 44	No skills transfer	3	5 days
ESI 44	Partial skills transfer	1	10 days
ESI 45	Commitment to comply with the Administrators' rules of professional conduct	5	Depending on the Service
ESI 46	Management of Administrator accounts not conform with the Safran Group security directive relating to the administration of IS	5	Depending on the Service
ESI 47	Compromised account or Contractor account not deactivated on mission completion	5	0 days
ESI 48	Administration privileges on the Buyer's IS with no prior formal validation by the Buyer's Security Department.	5	Depending on the Service
ESI 49	No depository for the Contractor's "Administrator" accounts	4	0 days
ESI 50	The Buyer's system administration platform is non-conform with the recommendations	3	Depending on the Service
ESI 51	Nonconformity of the technical means used for equipment operation and administration	3	Depending on the Service
ESI 52	Technical means and password management procedures non conform with Safran Group security principles	5	2 days
ESI 53	No encryption of Buyer information stored on mobile media used by the Contractor	2	5 days
ESI 54	Hardware maintenance and transfer operations non conform with Safran Group security regulations and the Buyer's security procedures.	2	5 days
ESI 55	No antivirus protection systems on the equipment administered by the Contractor	5	0 days
ESI 56	Use of software not subject to prior approval by the Buyer's Security Department.	2	Depending on the Service
ESI 57	Not applicable		
ESI 58	No implementation of the technical means for supervising and monitoring systems, managing disk areas and planning data processing operations	3	Depending on the Service

Reference of the requirement	Description of the risk (where several risks are linked to a given requirement)	Level of criticality	Bringing into compliance to a given deadline
ESI 59	No implementation of the means guaranteeing service continuity	3	Depending on the Service
ESI 60	Technical procedures covering system and equipment operation and administration do not correspond to the Buyer's needs or are not conform with good practices and security regulations	2	Depending on the Service
ESI 61	Security patches not applied to the systems and equipment that it runs and/or administers	5	2 days
ESI 62	Absence of or refusal to provide the evidence requested by the Buyer's Internal Audit Department	4	5 days
ESI 63	Nonconformity of the physical and environmental protection of systems and equipment	4	10 days
ESI 64	No monitoring of security activity and the regular review of events logs	4	Depending on the Service
ESI 65	Nonconformity of the procedures for managing accounts and access rights to equipment and systems	5	0 days
ESI 66	Organization noncompliant with the principle of the separation of privileges	4	5 days
ESI 67	Installation and configuration of IT equipment and infrastructure components conform with the recommendations	3	10 days
ESI 68	No performance of regular intrusion audits	4	Depending on the Service
ESI 69	Upgrading of systems and infrastructure components impacting on security without formal validation by the Buyer's Security Department	5	Depending on the Service
ESI 70	No computer system backup plan (PSI) set up for the systems operated and administered by the Contractor	4	10 days

Annex 1: list of applicable documents

The Security requirements are likely to be modified on a regular basis (changes to the documents below, addition of new documents, etc.). With each modification, the new version of the Security Requirements will be sent to the Contractor who agrees to comply with the new version in force.

The documents applying to the Service will be forwarded and studied during the contractualization phase.