

Confidentiality agreement


1% for Public Art Scheme – Doha

1% for Public Art Scheme within the framework of the construction of the new diplomatic campus in Doha, Qatar





This document sets out the aims and resources implemented to comply with the security conditions as required for the organization and operation of the Embassy of France in Doha, Qatar.

Documents, materials and information about the **1% for Public Art Scheme – Doha and the construction of the new diplomatic campus** are considered sensitive information and as such are subject to restricted circulation.

The following security clauses apply:

-  Information confidentiality clauses, security requirements and sensitive contract clauses, applicable to all supporting documents and information relevant to the project, and by all companies (design and works).

Any company involved in the **1% Public Art Scheme – Doha project** must declare that they have read and understood this document by returning a duly signed copy with their bid to the Ministry for Europe and Foreign Affairs along with following documents:

-  The company's own information security policy (antivirus protection, software updates, account access management, integrity of data flows, employee training, etc.), as well as the name of the company's information systems security manager (ISSM) if a person other than the company's managing director;
-  A list of employee names and copies of valid identity papers;
-  The register of instructions setting out the terms and conditions for work on sites of the Ministry for Europe and Foreign Affairs;
-  Individual declarations from employees accessing the work site.

SECURITY REQUIREMENTS

The company must describe the IT resources implemented as part of its process to continuously improve the security of its infrastructure and the mobile resources used, and specifically:

Antivirus protection

The company must provide a description of its antivirus policy applied to its IT systems and describe its procedures for and frequency of updates.

Software updates and security patches

The company must apply the patches recommended by hardware or software solution providers (system or application software, embedded software) to all the hardware for which it is responsible.

Data backup and restoration

The company must take all necessary measures related to data backup and restoration to comply with the required level of service.

Confidentiality and integrity of data flows

As a general rule, all data flows containing sensitive information and circulating on a public network must be encrypted using processes that guarantee confidentiality.

The company must describe all mechanisms and measures implemented to guarantee the confidentiality and integrity of data flows, such as the use of encryption tools for messages, files and collaborative tools.

Authentication

The company must describe its policy for IT account access management.

Employee training

The company must describe its policy on training employees in data security.

CLAUSES RELATING TO SENSITIVE CONTRACTS

The company, its employees and any subcontractors undertake not to divulge in any form whatsoever any data, information or documents of which they are or may become aware during the performance of the work under this contract and any amendments thereto.

The company undertakes to ensure that only individuals who have passed the basic checks required by law have access to the site where the work will be performed. No exceptions to the above provisions will be made, including to handle an unexpected, unintended or even urgent replacement of any of the company's employees.

1. List of employees

1.1 Prior to start of work

The company undertakes to submit to the contracting authority, prior to the start of work **a list of employee names** assigned to carrying out the work on the Ministry for Europe and Foreign Affairs sites, as well as the name, position and contact details of the on-site management staff.

This list must be kept up to date and include any changes in employees. No employees will be allowed on Ministry for Europe and Foreign Affairs sites unless they are on this list.







1.2. During performance of the work

The company undertakes to keep the list up to date and to indicate any employee changes.

The Ministry for Europe and Foreign Affairs may request that access to its site be denied and that the employee be replaced if the company has not informed the Ministry of the change in personnel.

2. Employee behaviour

The company undertakes to ensure that its employees:

-  exercise discretion,
-  comply with the sites' internal rules,
-  comply with safety and operational measures on the premises,
-  do not act in any way that is inappropriate with regard to the service,
-  do not carry or consume illicit products on the sites where work is performed,
-  do not use Ministry for Europe and Foreign Affairs equipment (e.g. telephones, vehicles, computers) for personal purposes, apart from the resources expressly made available to them.

The work must be performed in accordance with the conditions set out by the Ministry for Europe and Foreign Affairs, depending on the nature of the premises.



Before the start of work, the company undertakes to make available on the Ministry for Europe and Foreign Affairs site a register of instructions setting out the procedures for carrying out the work.

CONFIDENTIALITY CLAUSES

The company acknowledges that it is aware of the French General Interministerial Instruction no. 1300/SGDSN/PSE/PSD of 9 August 2021 on the protection of national defence secrets.

The company acknowledges that it has read Articles 413-9 to 413-12 of the French Criminal Code and that it shall not know or hold classified information.

The company must ensure that all personnel called upon under its responsibility in any capacity whatsoever to act on its behalf to perform the work sign an individual statement to certify:

-  they have read Articles 413-9 to 413-12 of the French Criminal Code;
-  they are not required, under penalty of criminal prosecution, to know or hold classified information.

The company undertakes to ensure that only people who have signed the aforementioned statement have access to the site where the work is to be carried out.

The company undertakes to submit the above individual statements to the Ministry for Europe and Foreign Affairs prior to any access by the relevant employees to the site where the work is to be carried out.

No exception to the above requirements may be accepted by or demanded of the contracting authority, including with a view to handling the unexpected, unintended or even urgent replacement of any of the company's employees.

Failure by the company to comply with these security measures, even if the result of carelessness or negligence, may result in a contractual penalty being applied, without prejudice to criminal penalties.

In (city):

Date:

Name of company representative:

.....

Signature:

.....