CHARTER FOR THE USE OF SCIENCES PO'S INFORMATION SYSTEMS

PREAMBLE

This Charter sets out the rules that must be respected in order to ensure that Sciences Po's Information Systems (IS) are used correctly, securely and in accordance with current legislation and regulations.

It applies to all Users of Sciences Po's IS and its aim is to:

- Guide each User to adopt the security practices necessary to ensure the optimum performance and security of Sciences Po's IS.
- Set out the principal rights, duties and responsibilities of Users of Sciences Po's IS, as per current legislation and regulations, as well as the rules and recommendations for accessing the Sciences Po Information System.

The principles set out in this Charter are supplementary to the application of French law and of all Sciences Po's internal regulations, particularly those concerning courtesy and respect for others. Hence, Users must treat their interlocutors appropriately and with the highest respect in interactions of any kind (email, discussion forums, social networks, websites etc.).

Users also have a duty to be sparing and economical in their use of IS and related Information, in order to avoid any unnecessary energy expenditure, the production of which is detrimental to the environment and the ecological transition. They must therefore destroy redundant or useless Information regularly, in order to reduce high energy-consuming stocks of data. Users must also ensure that they switch off their equipment when it is no longer in use.

Sciences Po shall use any method it deems suitable to bring the Charter to the attention of Users. Suitable methods include the following: distribution via the Internet, individual notification etc.

Users are reminded that, in the event of Improper Conduct, Sciences Po may decide to pursue disciplinary action, in accordance with the procedures applicable. These disciplinary measures will be undertaken independently of any legal proceedings that may or may not be instigated.

CHAPTER 1: GENERAL PRINCIPLES APPLICABLE TO ALL SCIENCES PO'S IS

Article 1 – Scope of application

The Charter applies to all Users of Sciences Po's IS. Sciences Po encompasses the following entities:

- The *Fondation nationale des sciences politiques* (FNSP).
- The *Institut d'Études Politiques de Paris* (IEP de Paris), including, where relevant, those mixed research centres within it that have access to Sciences Po's IS.
- The *Librairie des Sciences Politiques* LLC.
- The FNSP Press LLC.
- Sciences Po Services LLC.

Article 2 – Access to Sciences Po's IS

1. Management of access to Sciences Po's IS

Access to Sciences Po's IS and, where relevant, to the premises where they are housed requires use of one or more personal, confidential and non-transferable Means of Authentication. These means will be supplied to the User, who is responsible for ensuring their security and confidentiality.

Sciences Po issues the Means of Authentication to each User. The User must comply with the rules for storing and updating his/her Means of Authentication.

In particular, Users must refrain from:

- Noting the Means of Authentication on paper or electronically; storing it in a register, programme or non-encrypted file.
- Using or attempting to use any other Means of Authentication than their own and/or masking their identity.
- Using the Means of Authentication in a way that runs contrary to the Charter.

As a general rule, Users must not do or attempt to do any of the following: bypass the access control measures in place, gain entry to a system without permission or access Information and Resources that they are not authorised to access, as per Article 4 of the Charter.

2. Management of security breaches linked to the Means of Authentication

Without prejudice to the provisions of Chapter 3, in the event of any suspicion that a Means of Authentication may be compromised, Users must alert the IS Security Personnel and/or the Data Protection Officer (DPO) as soon as possible. They must confirm their suspicion in writing, by email, and request that the Means of Authentication be changed. Until this is done, the User remains responsible for any activity carried out under his/her identity, unless his/her good faith can

be demonstrated. As such, uses of IS made with a User-specific Means of Authentication are considered to have been made by the owner of that Means of Authentication, unless otherwise demonstrated.

3. Withdrawal of access

Users of Sciences Po's IS should note that their access may be suspended, restricted or re-examined by an Applications or IS Manager, for reasons of security or service requirements, including:

- When a User is no longer entitled to access Sciences Po's IS (termination of employment, completion of studies or service contract etc.).
- In certain cases of a permanent or temporary cessation of professional, educational or research activities.
- As soon as a case of Improper Conduct or Use has been detected.

In the latter two scenarios, the User will be informed in writing that one of the above measures has been taken. Users have the right to reply in writing.

Article 3 – Purposes of use of Sciences Po's IS

1. Use for educational, research or professional purposes

Use of Sciences Po's IS for these purposes is considered use made in the context of the User's professional, educational or research activities and within the scope of the authorisations granted to him/her.

2. Use for private purposes

Use of Sciences Po's IS for purposes outside of a User's professional, educational or research activities, i.e. in the context of his/her everyday or family life, is tolerated on an occasional basis, within reason and on the condition that this use complies strictly with all applicable laws and regulations, as well as with this Charter. Accordingly, the use must not:

- Be detrimental to the User's professional, educational or research activities.
- Have the potential to negatively impact the performance of Sciences Po's IS (disruption or limitation of technical capacities).
- Harm the interests or reputation of Sciences Po.

Hence, any files and messages that, at the time of their creation, processing or storage, have been clearly identified by the User as per the guidelines below, will be presumed private:

- **For messages:** both incoming and outgoing messages must contain an indication identifying them as private (e.g. "personal").
- **For files:** file names must contain an indication identifying them as private (e.g. "personal") and must be saved in specific directories that also indicate that they are private.

No professional, educational or research-related files may be named "private" or "personal".

In addition, any emails pertaining to trade union matters sent from or to the trade union's functional mailbox, a staff representative body or a trade union officer are considered private under the terms of this Charter, even if they are not explicitly identified as such.

Finally, any communications sent or received concerning activities protected by legal provisions (e.g. medical confidentiality) are also considered private under the terms of this Charter, even if they are not explicitly identified as such.

All other messages and files are considered to be professional, educational or research-related.

3. Withdrawal of access and private data

In the event that a User's access is withdrawn, as provided for in Article 2 of the Charter, he/she shall be informed 10 days prior to the withdrawal, except in the case of a withdrawal for security reasons or due to detected Improper Conduct or Use. It is the responsibility of the User to take steps to recover his/her private data within this period.

By way of derogation, Users engaged in trade union activities or belonging to staff representative bodies may, upon written request, be assisted by the DSI to recover any private data relating to their trade union activities.

4. IS security measures and private data

Users are informed that the automatic control measures and procedures implemented by Sciences Po for the purposes defined in Article 12 of the Charter, such as anti-virus software, apply to all incoming and outgoing messages and files, regardless of the presence or absence of an indication identifying them as private.

5. Improper conduct linked to the purpose of use of Sciences Po's IS

Unless expressly authorised by Sciences Po and enacted for educational or research-related purposes, any knowing use of Sciences Po's IS to collect, consult or attempt to consult, download, store, publish, share or distribute programmes, software, electronic documents, emails, information or data of the following kinds shall be considered Improper Conduct under the terms of this Charter:

- Violent, pedo-pornographic, xenophobic, racist, anti-semitic, Holocaust-denying, sectarian content and, more generally, any content contrary to current regulations.
- Content infringing respect for the human person, his/her integrity, dignity and private life.
- Defamatory content.
- Bullying, threatening or insulting content.
- Content that is clearly damaging to Sciences Po's internal or external brand image or reputation.
- Content inciting offences, crime and, more generally, any illegal activity or actions contrary to public order.
- Content contrary to public decency.

The above list is a reminder of the legislation in force.

Article 4 – Security requirements for Sciences Po's IS

As a general rule, every User is responsible for his/her use of Sciences Po's IS.

The Hardware supplied by Sciences Po guarantees optimum security and reliability. Accordingly, Users must never change or attempt to change the configuration and settings of IS or Hardware

supplied by Sciences Po, except with the express prior permission of the IS Security Personnel. This particularly applies with regards to:

- Downloading and installing software
- And/or network security devices.

Where necessary, the IS Security Personnel will conduct security checks of any changes or downloads proposed by Users with a view to granting such permissions.

In addition, to help preserve the security of Sciences Po's IS, Users must:

- Protect Sciences Po's IS by complying with any security regulations communicated to them.
- Be vigilant and alert the IS Security Personnel or, where relevant, their superiors if they notice any anomalies or any attempted or suspected violations of Sciences Po's IS. This should be done as soon as possible and in writing.
- Ensure that they do not allow any security breaches to enter the architecture of Sciences Po's IS and that they do not cause any disruption of the service.
- Not attempt to bypass the IS or Hardware security devices supplied by Sciences Po. In particular, they must not connect any Hardware allowing for wireless connection to the network without the DSI's permission.
- Not exploit or attempt to exploit potential IS security breaches, not publicise these, and not use the Hardware or Resources allocated to them in any abnormal ways.
- Refrain from storing, exchanging or allowing any Information to be processed by online services or service providers without the express prior permission of the IS Security Personnel.
- Understand and adopt best practices for the secure use of Sciences Po's IS, particularly as regards collaborative work, document sharing and password-related precautions. Users have a duty to make use of the appropriate services to keep themselves informed: website, guides, in person courses, online courses, SOS-helpdesk.

Article 5 – Information protection

The aim of Information protection is to ensure the availability, integrity and confidentiality of Information. It is vital for all users to be vigilant, since organisational and technical measures alone are not sufficient.

1. Duty of loyalty

The duty of loyalty applies to all Users of Sciences Po's IS. Hence, the following acts are considered Improper Conduct under the terms of the Charter:

- Distorting or using Information from Sciences Po's IS for the purpose of denigration; issuing false statements with the intention of falsifying Sciences Po's data.
- Responding to external requests attempting to obtain information relating to Sciences Po and its activities (telephone canvassing, emails, surveys etc.), without the express prior agreement of Sciences Po.

2. Duties of confidentiality and discretion

The User has a general and permanent duty of confidentiality and discretion in relation to the use of Information available on Sciences Po's IS. This is to safeguard the assets and interests of the institution and the persons concerned by this Information.

Accordingly, every User must:

- Be vigilant as to the risk of disclosing or publishing any Information used in the performance of his/her duties. This applies particularly to electronic communication and when using mobile Hardware outside of Sciences Po's premises (in hotels, public places, on transport etc.). Users are reminded that the confidentiality of digital correspondence, including via the Sciences Po email server, is reliant upon their own practices and vigilance. Hence, such correspondence must not be conducted without the appropriate security measures. Every User is responsible for safeguarding the confidentiality of his/her correspondence.
- Ensure that he/she does not make sensitive Information available to others without prior authorisation from Sciences Po.
- Avoid, other than when required for the performance of his/her duties and position, any use or communication of Information concerning or originating from Sciences Po, its partners, clients and staff, whether in oral or written form (press articles, publications on the Internet through forums or social networks etc.).

3. Duty to maintain the integrity of Information

The User must adhere to procedures for the hosting of Information, insofar as they are defined by Sciences Po. In particular:

- The User must regularly save the Information that he/she uses, creates or alters in the hosting spaces provided for this purpose. He/she is also personally responsible for backing up any data stored locally on his/her devices.
- The User must lock or disconnect his/her Hardware when leaving it unattended, even temporarily.
- The User must not move, duplicate or destroy any Information which his/her position and duties lead him/her to access without first ensuring that doing so will not be detrimental to Sciences Po.

4. Continuity of service

Without prejudice to the provisions set out above, in order to ensure continuity of service in the event that a User changes position within the Sciences Po community or leaves Sciences Po, he/she must follow the procedure for transferring the Information that he/she holds, for example in his/her shared spaces, email inbox or on Hardware supplied by Sciences Po. In particular, deletion of any Information that is not "private" must be subject to the general or specific authorisation of the DSI or the User's line or unit manager.

Application or IS Managers are authorised to back-up or archive all or part of Sciences Po's IS, including systems where Users' data is hosted, in order to ensure the continuity of service.

5. Vigilance and the duty to be trained in the secure use of IS

All Users are responsible for respecting the confidentiality of correspondence. It is therefore mandatory for all Users to be trained in the secure use of any Hardware and applications they use:

- Particular attention must be paid to collaborative work application suites and the email server.
- Users may make use of services provided by Sciences Po to obtain the necessary support and training: website, guides, specialised training services, recommendations.

Article 6 – Management of personal data

Automatic and manual processing of personal data is conducted on Sciences Po's IS as part of the institution's activities. The User is only permitted to process data for professional, educational or research purposes on Sciences Po's IS.

Any creation or modification of personal data processing procedures (including that resulting from the combination or interrelation of pre-existing data processing operations) is subject to the terms of current regulation regarding data protection and the relevant policies implemented by Sciences Po.

Any User who determines the purposes and means of the processing of the personal data, i.e. the objective and the way in which it is carried out, is considered to be operationally responsible for the data processing.

When a User is operationally responsible for the personal data processing, he/she must:

- Declare the personal data processing in the institutional data processing register, as required by the national and European regulations in force. Any attempt to reuse data for purposes not declared in this register constitutes Improper Conduct under the terms of the Charter.
- Obtain the written consent of the persons concerned.
- Follow the recommendations of Sciences Po's Data Protection Officer as far as possible and justify any measures taken in the event of non-compliance with these.
- Ensure that data is deleted and/or archived in accordance with the retention rules in force.

The User must inform Sciences Po's Data Protection Officer immediately in the event of a personal data breach.

Article 7 – Respect for intellectual property on Sciences Po's IS

Users shall not in any way use Sciences Po's IS to read, copy, store or transfer, without a license and for private or commercial purposes, any content or software protected by intellectual property law.

Users may not reproduce or use any third party files, data or databases protected by intellectual property law or private rights in any way that infringes the legal or contractual permissions granted to them.

Furthermore, as per the procedure defined in Article 4 of the Charter, any software authorised by the DSI must be used exclusively in accordance with the conditions of the licences obtained by Sciences Po. When using software distributed under a free licence, the User also undertakes to respect the terms of the corresponding licence.

Users are reminded that intellectual property such as photographs, images, databases, audio-visual and musical works, texts, logos etc. are protected by intellectual property law. The User must therefore not use the Resources (intranet, extranet, network etc.) in any way that infringes the intellectual property rights of Sciences Po or of third parties (illegal downloading, including from the Internet, unauthorised sharing of works protected by copyright etc.), including from the Internet, unauthorised sharing of works protected by copyright etc.).

CHAPTER 2: PRINCIPLES SPECIFIC TO CERTAIN USES OF SCIENCES PO'S IS

Article 8 – Mobile Hardware supplied by Sciences Po

In accordance with the rules set out in Article 4 of the Charter, Users must be vigilant when using mobile Hardware supplied by Sciences Po, particularly when connected to a network not controlled by Sciences Po.

They must also take certain specific precautions in order to prevent theft of the Hardware and loss of Information stored on it:

- Information stored on mobile Hardware must be backed up regularly, as per the conditions defined in Article 5 of the Charter.
- In all circumstances, the User must ensure that his/her mobile Hardware is secure, specifically by applying the security measures supplied by Sciences Po (e.g. attaching it to a desk with a security cable, keeping it in a locked cupboard or drawer etc.).
- Outside of Sciences Po's premises, the User must take care not to leave his/her mobile Hardware unattended (e.g. in hotel rooms, cars, public places etc.).
- In the event of loss or theft, the User must inform Sciences Po and/or the DPO as soon as possible.

Article 9 – Email server

1. General principles

Sciences Po provides Users with access to an email server. Inbox volume may be limited. Users may be permitted to exceed the volume limits on an exceptional basis.

In order to ensure that this email server is used appropriately for the exchange of information, in addition to the rules set out in Chapter 1, certain specific rules must be respected. These are as follows:

- The email server must not be used to send unwanted messages or spam.
- Users must not, under any circumstances, automatically forward messages to an email address other than the one provided by Sciences Po.
- Users must be vigilant as to the identity of the senders of messages received, particularly when receiving messages from external senders.
- Subscribing to external mailing lists is reserved strictly for professional, educational or research-related use. In addition, at the time of subscribing, the User must systematically check that there is a procedure for unsubscribing.

Users are also reminded that, with the exception of institutional mailing lists, the creation of a mailing list requires written consent from the persons concerned. Accordingly, it is mandatory to:

- Allow recipients on the mailing list to decline future messages ('unsubscribe' link included in all messages).
- Inform recipients on the mailing list of the nature of the message, particularly for messages pertaining to political or trade union matters (to be specified in the Subject line).

Article 10 – Use of online services

The increasing dependence of IS on online services (websites, discussion forums, social networks, file storage and exchange, online applications etc.) highlights new risks which require particular vigilance.

Accordingly:

- Use of these services must be undertaken in compliance with Sciences Po's rules and principles.
- As a preventive measure, Sciences Po implements a certain number of filtering procedures for websites, particularly those whose content may be contrary to public order or decency. Filtering of some sites may be removed upon the authorisation of the DSI.

CHAPTER 3: THE ROLE OF APPLICATION OR IS MANAGERS AND SECURITY MEASURES IN PLACE

Article 11 – IS security measures

1. Preventive measures associated with the use of Resources

Checks and monitoring measures are implemented in strict compliance with the principles of transparency and proportionality, solely for the purposes of security and the verification of proper access to and use of Sciences Po's IS.

The purposes of these measures are as follows:

- To guarantee the performance of Sciences Po's IS and maintain the continuity of service.
- To monitor compliance with rules relating to the use and security of Sciences Po's IS.
- To enable the detection and, if necessary, sanctioning of Improper Conduct or Use.
- To facilitate response to requests from authorised public authorities (police services, judicial authorities etc.).

To this end, the duties of Application or IS Managers include saving, backing up and managing digital footprints and event logs for Sciences Po's IS over the legal retention period.

In addition, for the sole purpose of raising awareness and training Users, the IS Security Personnel may organise simulated cyber attacks (phishing campaigns).

Finally, Users are informed that Application or IS Managers may access any IS at Sciences Po at any time in order to update, maintain, correct and repair Hardware supplied by Sciences Po and Resources required for IS use.

2. Corrective measures in the event of a security breach

Users are informed that Application or IS Managers may access any of Sciences Po's IS at any time in order to implement protective measures, which may include:

- Saving, storing or deleting Information collected and processed as part of Sciences Po's activities.

- Protecting the integrity and confidentiality of data and IS operation (dates of creation, sharing, receipt or deletion of Information, traces of intrusion into IS, in violation of the legal and regulatory provisions in place etc.).

In the event of Improper Conduct or Use, the IS Security Personnel may restrict or revoke rights to all or part of Sciences Po's IS (network, email, internet etc.) without prior notice. The User concerned shall then be informed in writing of the findings that prompted the intervention and may state his/her case.

Article 12 – Duties and role of Application or IS Managers

1. Rights of Application or IS Managers

The duties of Applications or IS Managers principally involve overseeing the quality and security of Sciences Po's IS. Application or IS Managers are responsible for the performance and security of Resources and the availability of Information and IS at Sciences Po.

In accordance with their role, Application or IS Managers may access Information relating to Users, under the conditions defined by the Charter and in compliance with the regulations applicable. In this respect, only Application or IS Managers are authorised to control Hardware supplied to Users by Sciences Po remotely in order to resolve problems reported to the DSI.

Only Application or IS Managers are authorised to add new Resources to Sciences Po's IS.

2. Duties of Application or IS Managers

Application or IS Managers are bound by strict duty of confidentiality.

Application or IS Managers are informed that they must respect the confidentiality of private correspondence and professional confidentiality, in accordance with the provisions of legislation and regulations in force. Specifically, Application or IS Managers are informed that:

- Messages sent to or from the inbox of an employee, non-permanent trade union representative or a member of a staff representative body (member of the CSE or elected member of an equivalent administrative committee) may, in the context of the corrective procedure provided for in Article 11.2 above, only be consulted subject to the agreement of the Secretary General and the head of his/her trade union organisation, in order to ensure that they do not relate to his/her trade union activity.
- Correspondence considered "private" as defined in Article 3 of the Charter is subject to the confidentiality of private correspondence and may not be consulted.

CHAPTER 4: ENTRY INTO FORCE

The present Charter is approved by the Boards of the IEP de Paris.

It was also approved by the Economic and Social Committee of the FNSP on 23 January 2020.

The Charter entered into force on 1 May 2020.

This document overrides and replaces all previous documents of the same nature issued by Sciences Po in relation to the use of Sciences Po's IS.

CHAPTER 5: DEFINITIONS

Words capitalised within the Charter are defined as follows.

"Charter": refers to the present document.

"Improper Conduct/Use": refers to conduct or use running contrary to the Charter and/or applicable rules or laws.

"Data Protection Officer (DPO)": refers to the staff member at Sciences Po appointed to inform, advise, support and monitor the institution in matters relating to the protection of personal data and the privacy of members of its community. Hence, by virtue of his/her duties, the Data Protection Officer has access to all information relating to data processing operations at Sciences Po and the persons concerned by these. He/she is bound by a duty of confidentiality. He/she provides training and raises awareness among the various communities concerned, specifying that he/she may also be called the Data Privacy Officer. At the time of adoption of the Charter, the need for this post is stipulated in particular by EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Information Systems Department (DSI)": refers to Sciences Po's *Direction des Systèmes d'Information,* the department responsible for the development, technical implementation and operational and security maintenance of Sciences Po's IS.

"Hardware": refers to all fixed or mobile hardware allowing Users to access Sciences Po's IS and/or process Information relating to Sciences Po locally on the Hardware (fixed computers, laptops, mobile phones, smartphones, tablets etc.).

"IS Security Personnel": refers to the personnel at Sciences Po who are responsible for defining and monitoring the effective application of rules ensuring the security of Information and IS. The team is composed of the IS Security Manager(s) and associated staff at the DSI.

"Application or IS Manager": refers to the Users responsible for installing programmes and monitoring their use. Application or IS Managers have a higher level of access to Sciences Po's IS, which allows them to manage and control all or part of their operation.

"Information": refers to an item of knowledge (data, sound, still or moving image etc.) that can be stored, processed or shared through a defined coding system and by way of a physical (paper) or electronic (dematerialised) medium/document.

"Means of Authentication": refers to any element or set of elements enabling a User or Resource to prove his/her/its identity in order, for example, to be granted access to Information or an IS (password, smart card and corresponding activation code, encrypted double key and associated digital certificate etc.)

"Resource": refers to any item (material – printer, servers, network –, software, application, procedures, settings etc.) involved in the implementation and operation of an Information System.

"Sciences Po": refers equally to the *Fondational Nationale des Sciences Politiques* and/or the *Institut d'Études Politiques de Paris*.

"Information Systems (IS)": refers to all technical means used to process information. The structure of an IS is composed of all Hardware and Resources organised in such a way as to collect, store, process and communicate Information, by means of the User's Hardware.

"User": refers to any person of any status (student, guest, staff member of the FNSP or the IEP, service provider, board member etc.) who accesses and/or uses Hardware, Resources, IS, Information on a continual or occasional basis.

Signed:

Paris, 1 May 2020

Frédéric Mion, Administrator of the *Fondation nationale des sciences politiques* and President of Sciences Po