IT CHARTER

Introductory comments

A. Summary

The Charter governing the use of information technology (IT) resources is addressed to users of the IT resources provided by Doctors of the World - Médecins du Monde (MdM). This Charter defines the rules governing the use of these IT resources and must be complied with by all users. It sets out the responsibilities incumbent upon each user and informs users about the controls put in place by MdM to guarantee the security and effectiveness of its IT Systems.

This IT Charter represents the essential factors governing the use of the IT resources; it may be completed by charters specific to certain tools, notably regarding the use of the IT tool designed for the management of medical data, the use of Wi-Fi by guests or temporary visitors MdM's headquarters, etc.

This Charter will be submitted to MdM's employee representative bodies and circulated by the Human Resources Directorate to all users at MdM.

B. Updating Rules

This document must be reviewed at least once a year by the IT Department. It must cover:

- **Internal events**, notably: changes to the missions of MdM, developments concerning the structure, developments regarding the IT system's technical or application architecture;
- **External events**, notably: changes to the legislation, developments regarding contracting policy, new threats or challenges, new partners;
- **Improvements identified** in the context of the monitoring and audit procedures implemented.

C. Purpose

MdM's IT resources are a work tool that is made available to users to enable them to perform the assignments entrusted to them by MdM. **The correct use by users of these IT resources is vital to ensure their duration.**

Any inappropriate use of the IT resources can entail serious consequences for MdM, such as:

- **MdM having legal liability**

In the event of any unlawful use or damage caused via its resources by one of its employees or volunteers, MdM may be found liable and legal proceedings launched against its executives;

- **Loss of confidentiality**

An error in the name of the person to whom an email is being sent, a copy of confidential information stored on a resource that is not properly protected or the theft of a laptop and the information that it contains are a few examples of the threats that could jeopardise the confidentiality of the information held by MdM;

- **Damage caused to the image and reputation of MdM**

A poorly written message, containing offensive, unlawful or inappropriate comments could have a significant impact on the image and reputation of MdM;

- **Loss of efficiency**

Any inappropriate use of resources such as Internet access or email may lead to a loss of user efficiency (important number of irrelevant messages to be processed, infection with a computer virus, saturation or slow Internet and email speeds, etc.).

This Charter aims to reinforce users' level of awareness and responsibility regarding the correct use of the IT resources provided to them by MdM.

The Charter defines, in accordance with individual and collective freedoms:

- users' rights and obligations regarding the use of IT resources;

- the context for the use of the resources on a professional basis[1] and the conditions associated with personal use;
- the methods used by MdM to guarantee control over access to, and use of, the IT resources;
- what to do in the event of an incident linked to the IT system.

This Charter does not aim to provide exhaustive cover of all possible situations. It is not meant to replace the relevant legislative and statutory provisions. It sets out the expected principles of use with regard to the IT resources.

D. Scope of Application

This document applies to **all users of the IT resources** provided by MdM.
IT resources here means all IT tools and equipment (software, applications, computer workstations, servers, data storage supports, etc.), information irrespective of the storage method and all means of communication linked to this information (telephone, fax, email, Internet, Intranet, forums, etc.).
Users means all MdM stakeholders including MdM employees (permanent or temporary employment contracts), temps, interns, external service providers as well as volunteers, members and elected delegates of MdM.
This document does not apply to beneficiaries and users of the services provided by MdM.

E. Responsibilities

Each user is responsible for the IT resources used by him and must, on his or her level, guarantee their protection to ensure that such resources remain available, secured and high-performance. **Each user makes a commitment to comply with the principles and rules detailed in this Charter.**
Managers, unit heads and regional delegates must ensure that this Charter is properly circulated and applied within their teams. They must forward this Charter and its content to all users under their remit.
The Charter is provided as an appendix to all MdM employment contracts and internship agreements, so that each user has access thereto. It is attached as an appendix to all agreements covering the provision of services and partnerships that involve the use of MdM IT resources. The charter applicable to volunteers and members of MdM makes reference to the Charter which is available to volunteers via the Intranet.

[1] In this document, "professional use" means all activities carried out by employees, volunteers, interns, members of the organisation and service providers, carried out in the name of MdM and on its behalf.

Rights and Duties

1. GENERAL CONDITIONS

1.1 Access Authorisation

Access for user to MdM's IT resources is subject to approval from a management superior for employees, from the relevant regional delegate or activity manager for volunteers, from the individual responsible for any assignment entrusted to an external service provider, and from the internship supervisor for interns.

1.2 Professional and Personal Use

MdM's IT resources are provided to users to enable them to perform the assignments entrusted to them by MdM.

A reasonable level of personal use of MdM's resources is tolerated when within the context of the needs of day-to-day life, and on condition that such use does not constitute an obstacle to use for professional purposes. The use of the IT resources provided by MdM for personal purposes leads users to assume full civil and penal liability for such use of the IT resources.

Information for personal use must be marked clearly and unambiguously as being "**for personal use**" or in similar terms; information for personal use may be stored via physical or cloud storage named "personal use" or similar, or kept in files marked "for personal use"; all messages for personal use must be marked in their object as being "for personal use" or similar, or must be stored in a file named "for personal use".

Any information not stored in this manner shall be considered as being for professional use.

1.3 Compliance with the National Legislative Framework: Banned or Immoral Information

It is **strictly prohibited** to deliberately store, send or forward any information that is immoral and/or banned by the legislation in force, unless such information has a direct link to the work being carried out and is not contrary to public order, notably information that:

- is of a violent nature, pornographic or liable to harm the dignity, honour or integrity of human life, as well as contrary to the protection of minors;
- is likely to encourage others to perpetrate crimes and offenses, to promote the use of banned substances, discrimination, hatred or violence;
- makes an apology for crimes against humanity or terrorism;
- constitutes harassment or bullying in any manner whatsoever;
- is defamatory, insulting, vulgar, obscene, threatening to the privacy of others;
- violates the legislation and rules in force regarding intellectual property: users are prohibited from copying or illegally using any software or information protected by a license, copyright or any other ownership rights.

1.4 Protection of Personal Data

In accordance with French law 2004-801 of 6 August 2004 on the protection of natural persons with regard to the processing of personal data, any plan involving the creation, processing, storage and circulation of personal data must be submitted to the MdM Data Protection Officer prior to implementation. These declarations are handled exclusively by the Data Protection Officer within the Legal Department of MdM: juridique@medecinsdumonde.net/blandine.contamin@medecinsdumonde.net

1.5 Compliance with Foreign Law

The software installed on the computer workstation complies with the rules of use determined by French law. Users must ensure that all useful measures are taken in the event of travelling abroad in respect of software user rights. Such precautions concern more specifically the use of encryption tools or electronic signature tools that may be regulated abroad. They also relate to surfing the Internet, which is filtered in some countries. Information must therefore be obtained first from the security officer and/or legal advisor at your disposal.

2. PROTECTING EQUIPMENT

Users are responsible for protecting any equipment provided to them by MdM.

2.1 Approved Equipment

Only equipment that has been provided and approved by the IT Department or the local IT team can be installed and connected to the MdM internal networks and computer workstations.
In this document, local IT team means:
- for users at headquarters: the IT support provided by the IT Department;
- for users in the regions or internationally: the individuals in charge of computer workstation maintenance within the relevant structure.

2.2 Configuration Changes

In order to maintain an appropriate level of security, users must never change the configuration of computer workstations or of any other equipment provided by MdM.
In particular, users must not:

- add or remove any hardware (hard drive, network card, etc.) that is not in line with instructions from the MdM IT Department or local team;
- uninstall or deactivate any security software or mechanism (virus prevention software, firewall, password parameters, installation of security updates, etc.);
- download and install any software that has not been validated by MdM. A request must be made to the local IT team before installing any non-validated software. This team will then validate or have validated the software item (licences, technical impact on configuration, maintenance and support, etc.) before proceeding with this installation.

Any user who has a laptop provided by MdM must log on to the MdM network on a regular basis to ensure that the device's security measures are updated regularly. Please note that the laptops provided by MdM cannot be used other than by MdM staff.

2.3 Physical Protection

In order to limit the risks of the equipment provided being stolen or lost, users must in particular take care to ensure:

- the use of the protection methods provided to guarantee the protection of any "mobile" equipment (laptops, PDAs, mobile phones, etc.) and related accessories (USB sticks, removable hard drives, batteries, etc.): to be kept in a lockable drawer or cupboard, use of security cables, etc.;
- that equipment is not left unsupervised in areas to which access is not restricted: users must be particularly vigilant in public places and on public transport.

3. DATA PROTECTION

Users have a duty to protect all of the information stored on the IT resources provided (internal hard drive, laptop, removable hard drive, USB stick, CD or DVD, etc.). Users must act with discernment and comply with the data protection and classification rules established by MdM.

3.1 Access Rights

The accreditation (account and password) for access to the MdM IT Systems established for each user is strictly personal and cannot be assigned, temporarily or otherwise, to any third party, even managers (except under the specific circumstances described in this section).

Users must take all measures necessary to limit fraudulent access to IT resources and on this basis must notably:

- ensure that all user accounts, together with all codes, passwords, cards, keys or other access control methods entrusted to users on a strictly personal basis, are kept confidential, in particular by not displaying passwords. The password chosen by the user must be made up of at least 10 characters of different kinds (numbers and letters) and be updated every 6 months. An automatic password update reminder is sent to each user and assistance is available from the IT Department.
- Never lend, sell or assign user accounts, codes or other access control methods or allow their use by a third party;
- lock or close all sessions on the computer workstation in the case of absence, even momentary;
- ensure that all files considered as confidential are protected against third party access.

Access to the computer workstation is obtained on the basis of the identification and authentication data provided by MdM.

Users must not use or try to use any IT resources to which they have not been given access rights. Users must not use a false identity or conceal their actual identity.

3.2 Document Protection

Users must do their best to adopt behaviours aimed at ensuring a level of security that corresponds to the sensitivity of the information and resources used and, in particular:

- when using removable supports (hard drives, USB sticks, etc.) and portable equipment (laptops, mobile phones, etc.), ensure their physical protection (in a safe) or use the sensitive data encryption software provided with these supports;
- back up all local data to the user's computer workstation on a regular basis; these back-up copies must themselves comply with the rules ensuring the confidentiality of the relevant data;
- delete all data no longer required;
- empty the computer's recycle bin and temporary folders on a regular basis: computer workstation recycle bin, web browser history, Internet cookies, etc.;
- manage printing on the basis of sensitivity and pick up any sensitive documents immediately from printers, fax machines and photocopiers.

4. USING MEANS OF COMMUNICATION

Content obtained over the Internet is rarely guaranteed with respect to its quality, legal status and right to be used for professional purposes. Users must demonstrate the greatest possible vigilance regarding the confidentiality, integrity and reliability of all elements sent, received or read on the Internet.

4.1 Access Conditions

Access to electronic communication resources from the MdM internal network is provided exclusively through the means provided by MdM. Connecting any other kind of external access method (such as a Wi-Fi access point, external network gateway, etc.) to the MdM network is prohibited.
Users must be authenticated before accessing the Internet or the messaging service. Authentication data (password, confidential PIN, etc.) **is strictly personal** and users are responsible for keeping this data confidential.

4.2 Messaging Service

As stipulated in the section “Professional and Personal Use”, personal messages must be kept clearly separate. A message is considered as being personal:

- if the subject line contains the word “**personal use**”;
- or if it is stored in a physical or cloud folder named “**personal use**”.

Users are responsible for assessing whether a message is “personal” or not.
When sending a “personal” message, users must ensure that the content of the message cannot mislead the recepient regarding the personal nature of the message. Users must not use their professional signature in this case. As a reminder, employees must ensure that all content complies with their duty of loyalty to their employer.
Please note that for all messages not secured via specific encryption methods, the security provided by the web-based messaging service is comparable to sending a postcard.
Anyone can read the message and there are no guarantees as to either the time taken for delivery or the delivery itself.
When sending a professional message, users must therefore act with discernment and protect any non-public information sent via email by referring to the classification and protection rule established by MdM.
Moreover, users must not:

- send any messages whose content could be harmful to the image or reputation of MdM, in particular in the context of exchanges with partners or donors;
- send or forward any unrequested mail ("spam"[2]), messages containing unlawful or offensive messages, or any “chain”-type emails;
- unless validated by MdM, set up any rules for the automatic forwarding or sending of any messages sent to the user to a non-MdM email address;
- change any message received from a third party without indicating that changes have been made before forwarding the same;
- read any information to which the user does not have access rights.

These provisions apply more specifically to any email not sent directly or copied to the user.
The sending of messages to all MdM **users or all users within a single structure is in principle prohibited, unless specifically authorised. The authorisation procedure must be defined in the rules applicable within each structure.**
Users must be vigilant with regard to any messages received. To this end, users must not:

- open any messages when the origin, subject or content is uncertain;
- save and run any suspicious attachments;
- make any significant decisions on the sole basis of an email. In case of doubts, users should contact the sender of the message or, if not possible, the local IT team to confirm that the information received is accurate and authenticated.

Subscribing to external email lists using a Médecins de Monde email address is permitted for professional purposes only. When joining such lists, users must systematically check that it is possible to unsubscribe.

[2] "Spam" means any electronic communication, notably email, not requested by the recipients, sent in mass mailings as advertising or for dishonest purposes.

4.3 Navigation

A reasonable level of use of Internet access is allowed when part of the needs of day-to-day life, and on condition that such use does not act as an obstacle to use for professional purposes.
Users must be particularly vigilant when surfing the Internet; they are in particular prohibited from:

- looking at, downloading, forwarding or saving any content that is illegal or harmful to the image of MdM; in the event of accidental access to an illegal website or a website not authorised by MdM, users must quit the page immediately;
- disclosing their personal ID on the websites looked at;
- disclosing their contact details - in particular, their email address - on any websites that are unconnected to their professional work and the image of which would be incompatible with the image of MdM.

The launch of any online communication tool (a professional chatroom or community or a website) by a user in the capacity of a representative of MdM or of any of its entities must be authorised by management and notified in advance to the Communication and Development Directorate and the Legal Department of MdM.
Taking part in any forums, blogs, chat groups or social media networks on a professional basis, in the capacity of representative of MdM is also subject to the same conditions.
When using these online communication tools, users must ensure that, as representatives of MdM, they are complying with media rights, professional confidentiality rules and respect for privacy, notably regarding the publication of photos, and that they follow all MdM internal instructions and rules.
Users are however reminded that they are acting in the name of MdM and must therefore ensure that they are not harming the interests of the organisation. If in doubt, users must contact the MdM Communication Directorate in advance.
In the context of the use of instant messaging on a personal basis or of participation in chatrooms, blogs, forums or social media networks on a personal basis, users must without fail use a personal email address.
Users must ensure that the content of any messages does not generate any confusion as to whether they are speaking on behalf of MdM or as to whether the message has been drafted in the context of the performance of their official duties. In particular, users must never use the MdM symbols or logos.
This provision does not release users from their duty to act with discretion and care.

4.4 Using Your Own Equipment

The email account can be configured on a user's personal mobile phone or computer. MdM cannot however be liable for any damage caused by such use to the equipment. The MdM IT Department has no obligation to provide assistance in relation to such personal equipment. Should the IT Department help with personal equipment, it has no liability whatsoever regarding any potential damage caused as a result.
Agreeing to install the email account on certain mobile phones may give the IT Department access to the content of this phone so as to be able to delete MdM data if the account is removed. A message asking the user for validation is in this case displayed when setting up the account on the phone.

5. MONITORING AND DATA GATHERING

In order to guarantee the proper technical operation and security of its IT Systems and to protect its interests, MdM reserves the right to limit, analyse and monitor usage footprints via equipment resources and software, together with any exchanges, whatever their nature or subject, made via its IT Systems.
In this context, MdM in particular uses logs which record traces of certain actions by users.

The monitoring and analysis actions implemented by MdM are carried out when abnormal behaviour has been detected or in the specific cases allowed by law. These actions are not intended to carry out the systematic monitoring of each user.

These monitoring and analysis actions are exclusively carried out by IT administrators in accordance with the legislation applicable and in particular with French data protection law (loi Informatique et Libertés). The IT administrators are bound by rules regarding the confidentiality of any information that may be disclosed to them in this context.

6. FILTERING AND RESTRICTIONS

Technical restrictions used to filter access to the Internet are used to limit web browsing options. The principles that govern MdM as well as the regulatory framework are used to determine the restrictions imposed. The use of these filters does not release users from their responsibilities.
Email accounts are subject to technical restrictions concerning the size of any files sent and the extensions of certain files.
Internet and email access is subject to antivirus protection that may, as a safety measure, restrict access to a given website, delete email attachments or remove the content of specific emails.
These measures are vital to ensure the safety of external access. MdM cannot be held liable for any data loss as a result of these controls or the consequences thereof.

7. MONITORING METHODS

7.1 Specific Measures for Email Accounts

The information saved in the email logs is:

- message sender;
- message recipient;
- date and time at which the message was handled.

➔ **These logs are kept for 90 days.**

MdM reads the "envelope" of certain messages (date, time, from, to, subject, etc.). If the subject of the message does not indicate that the message is private and if the user has failed to comply with the general measures set out in part 4.1 above, the content of the message may be read.

7.2 Specific Measures for Internet Access

The information saved in the Internet access logs is:

- website address (URL);
- ID used for the connection may also be recorded;
- flow type (HTTP, FTP, etc.);
- volume of data received and sent.

➔ **These logs are kept for 30 days.**

MdM abstains from using this information to monitor which websites are being looked at by employee and union representatives in the context of the activities linked to their official position.

7.3 Specific Measures for Access to Shared Resources

The information saved in the logs for each case of access to shared resources (network readers) is:

- date and time of the connection;
- ID used for the connection;
- profile associated with the connection (privileges allocated).

➔ **These logs are kept for a maximum of three months.**

The content of any non-private files may be read. In this case, MdM may inform the user in writing that the data has been read.

7.4 Specific Measures for Computer Workstations

The information saved in the computer workstation logs is:

- details of log-ins to the computer workstation: IDs used for successful and failed log-ins;
- details of any "system errors" identified on these computer workstations;
- details of any incidents flagged by the virus prevention software on the computer workstation;
- details of any incidents flagged by the personal firewall for those computer workstations on which this has been installed: blocked flows, incidents detected, etc.

➔ **These logs are kept for a maximum of three months.**

The content of any non-private files may be read. In this case, MdM may inform the user in writing that the data has been read.

7.5 Specific Measures for Remote Access to the IT Systems

The information saved in the logs recording each remote connection to the MdM IT Systems is:

- date and time of the start and end of the connection;
- ID used to connect.

➔ **These logs are kept for a maximum of six months.**

7.6 Specific Measures for Restricted Access Applications

The information saved in the applications logs is based on the legal and statutory requirements applicable to each application.

By default, the following information is saved:

- User ID, plus access profile if applicable;
- date and time of the connection.

➔ **These logs are kept for three months by default.**

For applications that do not apply these default rules, details regarding the information saved, its purpose and the retention period will be provided to users of the application.

7.7 Specific Measures for Landline Telephones

The information saved in the logs covering internal telephone infrastructure (telephone switchboard, IP phones) or provided by the operator used by MdM is:

- telephone number called[3], service used, operator called, destination of the call (local, regional, national or international call, premium rate call);
- call length, date and time of the call start and end, billing details (number of taxes, volume and type of any data exchanged excluding data content, and cost of the service used).

➔ **These retention period lasts for no more than one year starting from the date from which charges for the telephone services are billed.**

A detailed list of calls made from a specific telephone can be produced. Such a list will only be provided further to a specific, reasoned request (evident abnormal use of the telephone) from the manager or financial manager in the event of abnormal charges within the division or mission of the individual in question. Such individual must be given access to this list and be given the opportunity to provide an explanation to his manager.

MdM abstains from using the information obtained in relation to telephone use in order to check calls made and received by employee union representatives in the context of their official position.

7.8 Access to Users' Computer Workstations, Files and Emails

[3] The numbers called are indicated by the final four numbers only.

In the absence of the user

If a user refuses or is unable to provide the information necessary for the continuation of MdM's activities and if such information is not available via any other means, his managers within the division or mission head may ask the local IT team to obtain access to those resources necessary for the continuation of MdM's activities. **These exceptional requests must be reasoned and formalised by the party making the request to the Human Resources Directorate, which then forwards the request to the IT Department after consulting with the elected employee representatives. For a member of the HR Directorate, the request must be made to the Directorate General.**

In this case, MdM is prohibited from accessing the user's personal data, as defined herein.

Departure of the User

When a MdM user leaves the organisation, for any reason whatsoever, the account closure methods applied are as follows:

- the user's manager, division manager or mission head asks the local IT team to close the user's accounts, indicating the desired date (a period for information is provided in the note on the management of email addresses, see Appendix A);
- the user's manager gives this closure date to the user;

the user's manager, division manager or mission head may ask the user, prior to his departure, to provide all information necessary for the continuation of MdM's activities. If the user refuses or is unable to provide this information, and on condition of it being impossible to access this information via any other means, the manager, division manager or mission head may ask the local IT team to provide this information after the user has left.

These exceptional requests kind must be reasoned and formalised by the party making the request to the Human Resources Directorate, which then forwards the request to the IT Department after consulting with the employee representatives. For a member of the HR Directorate, the request must be made to the Directorate General.

In this case, MdM abstains from accessing the user's personal data, as defined in this section. The user is however advised to delete all personal data prior to the date on which his accounts are scheduled for closure. The account will be deactivated and then deleted after the recovery of any documents and emails.

Access to Personal Data

MdM reserves the right to authorise access to personal data in the event of:

- a clear and present danger threatening the interests of MdM and that can be classified as a state of necessity;
- reasoned requests from the competent legal authorities or the police, with the approval of the Legal Department at MdM's headquarters.

Access will be granted to this information in accordance with the principle of due proportion and in accordance with the law, in particular, with respect to privacy of correspondence and personal privacy.

Other than in such cases, all access to the content of a file, folder or message that has been specifically tagged as being for personal use must be carried out in the presence of the user or after having invited the user to attend.

8. ACCESS DENIED

In the case of any unlawful or unauthorised use or any use that jeopardises the correct functioning of the IT Systems, the security of the IT Systems or the interests of MdM, the IT Department or the local IT team may implement any specifically tailored protection and/or correction action necessary until normal service is resumed, and inform management of this fact.

Users' access rights to the IT resources may be modified or withdrawn at any time by MdM.

Internet and email access may be suspended, restricted or removed, individually or collectively, via technical or administrative measures, when necessary, notably to ensure the correct functioning and integrity of

MdM's IT Systems.
These measures may be implemented without users having been informed in advance. Behaviour in the event of an incident.

9. LOSS OR THEFT OF A RESOURCE

If any IT equipment (computer workstation, removable device, etc.) provided by MdM is lost or stolen, users must:

- inform the manager, division manager or mission head and the local IT team, and provide them with:
  - details regarding the circumstances of the loss or theft, to allow MdM to decide on the interest of launching proceedings in the name of MdM; users must not launch proceedings in their own name; only an authorised representative is able to launch proceedings in the name of MdM;
  - an inventory covering the data held on the equipment, together with the corresponding level of security and level of protection as of the time of the loss or theft;
- the local IT team will forward this information to the IT Department at headquarters and the Data Protection Officer within the headquarters Legal Department.

10. INFECTION OR INTRUSION INVOLVING A COMPUTER WORKSTATION

If the occurrence of an event that could harm the MdM IT Systems is suspected or acknowledged (for example, intrusion or infection by malicious code on a computer workstation or IT resources), users must not try to solve the problem themselves.
Users must:

- isolate the piece of equipment by disconnecting it from any network used and notably the MdM network;
- inform the local IT team, which will then take all measures necessary to limit and resolve the incident.

Infection by malicious code (viruses, worms, spywares, Trojan horses, logic bombs, etc.) or intrusion via computer workstation may be flagged up by the abnormal behaviour of equipment and alarms triggered on security equipment (antivirus software, personal firewall, etc.).
The Data Protection Officer within the Legal Department must be informed by the IT Department about any failure having endangered the protection of MdM personal data.

11. EQUIPMENT MALFUNCTIONS

If equipment malfunctions or if the aforementioned requirements have not been met, the decision may be made to proceed with a complete reconfiguration of the system.
If applicable:

- the local IT team will reboot the equipment with its initial standard configuration;
- the local IT team will not restore any data marked as "private". MdM shall have no liability with regard to the loss or distortion of any data marked as being private, or the consequences thereof.

APPENDIX A: Timescale for the deletion of email accounts after the departure of the user

This timescale is taken from the note entitled “Process for the creation and deletion of email accounts v1.0” dated December 2013:

- for interns and volunteers: on the date that their contract comes to an end;
- for employees: 1 month after the date that their contract comes to an end;
- for mission heads, group heads, regional delegates, regional secretaries and regional treasurers: 3 months after the registration of the individual’s resignation/end of appointment by the Board;
- for directors: 12 months after the expiry of their appointment;
- for Bureau members: 24 months after the expiry of their appointment;
- for former presidents: 36 months after the expiry of their appointment;