Politique de gestion des traces d'utilisation des moyens informatiques et des services réseau au CNRS

1 - Contexte

Le fonctionnement du CNRS passe par l'utilisation de systèmes d'information et de moyens de communications modernes et de plus en plus performants, qui s'appuient sur des réseaux télématiques connectés à l'échelle mondiale. Ces réseaux, qui apportent une souplesse inégalée, ont également une grande vulnérabilité intrinsèque, et leur utilisation engage la responsabilité personnelle des utilisateurs, ainsi que celle de notre organisme qui met ces moyens à leur disposition en temps qu'outil de travail.

L'utilisation des nouvelles technologies de communication pose le problème de la protection d'une part de l'information sensible[1] gérée par les utilisateurs et d'autre part des systèmes d'information sous la responsabilité des laboratoires. Les mesures mises en œuvre doivent permettre au CNRS de remplir ses missions tout en satisfaisant aux exigences qui sont imposées par ses engagements vis-à-vis de ses partenaires, de la réglementation sur la protection des données sensibles et la protection du patrimoine scientifique, et de la loi sur la protection des données personnelles, nominatives et la sécurité des systèmes d'information. Cette protection doit être mise en œuvre dans le respect du droit de l'individu à la protection de ses informations personnelles.

Une déontologie et un contrôle de l'utilisation sont donc nécessaires, de même qu'une information et une sensibilisation des personnels. Le CNRS a défini une politique et mise en place des dispositions et moyens pour assurer la sécurité et le contrôle de l'utilisation des moyens télématiques et informatiques, et d'autre part il a fixé les conditions d'utilisation de ces moyens, afin de garantir les droits individuels de chaque agent.

Cette politique doit aider les responsables du traitement informatique à s'assurer que :

- La collecte des informations n'est ni frauduleuse, ni déloyale, ni illicite et qu'elle s'accompagne d'une bonne information des personnes ;
- Les informations ne sont pas conservées au-delà de la durée prévue ;
- Les informations ne sont pas communiquées à des personnes non autorisées ;
- Le traitement ne fait pas l'objet d'un détournement de finalité ;
- L'accès aux résultats des traitements et aux données collectées fait l'objet d'une sécurité optimale, afin qu'aucun détournement de la finalité ne puisse avoir lieu.
- Les applications à caractère nominatif font l'objet de demandes d'avis préalables

[1] Informations sensibles au sens ou la confidentialité (contrat, données de recherche, information nominatives, ..), l'intégrité (…., informations de gestion) et la disponibilité nécessitent une protection particulière.

à la CNIL

Cette politique est applicable à l'ensemble des unités du CNRS. Chaque unité est responsable de sa mise en œuvre, sous la responsabilité des instances de pilotage de la sécurité des systèmes d'information au CNRS et en particulier du Fonctionnaire de Sécurité de Défense de l'établissement.

2 – Mise en place d'une gestion des traces dans les unités du CNRS - principes de base -

Une maîtrise de la sécurité de fonctionnement des systèmes d'information et une garantie de la licéité des transactions opérées nécessitent un contrôle s'appuyant nécessairement sur l'enregistrement systématique et temporaire d'un certain nombre d'informations caractérisant chaque transaction, appelées traces.

Ces traces ont plusieurs objectifs :

- La métrologie du réseau : contrôler le volume d'utilisation de la ressource, détecter des anomalies afin de mettre en place de la qualité de service, faire évoluer les équipements en fonction des besoins ;
- Vérifier que les règles en matière de SSI sont correctement appliquées et que la sécurité des systèmes d'information et du réseau telle qu'elle a été définie par la politique de sécurité de l'unité est assurée ;
- Détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ;
- Détecter toute violation de la loi ou tout abus d'utilisation des moyens informatiques pouvant engager la responsabilité du CNRS ;
- Être à même de fournir des preuves nécessaires pour mener les enquêtes en cas d'incident de sécurité et de répondre à toute réquisition officielle présentée dans les formes légales.

Les traces à enregistrer de manière systématique portent sur l'utilisation des moyens suivants :

- Les serveurs et postes de travail ;
- Les équipements d'extrémité de réseau et la surveillance des services réseau (routeurs, pare-feux, …) ;
- Les équipements de surveillance du trafic réseau (IDS, antivirus, antispam, ...) ;
- Les applications spécifiques.

Des durées maximales de conservation sont indiquées pour chacun de ces types de traces. En revanche, les durées minimales de conservation sont laissées à l'appréciation des gestionnaires du système. Elles pourront, en fonction de l'évolution de la législation, être précisées dans des textes ultérieurs.

Les objectifs précités imposent d'aller au-delà d'un enregistrement et d'une exploitation de données statistiques. Ils impliquent nécessairement l'enregistrement, la conservation

temporaire et l'éventuelle exploitation de données nominatives, dans la mesure où des éléments contenus dans les traces permettent de remonter à l'utilisateur.

Ces traces et leur traitement doivent également respecter les droits de chacun et notamment être conformes à la loi du 6 janvier 1978 dite "Informatique et libertés". Elles doivent avoir satisfait au principe d'information préalable et de transparence.

Le présent document fait partie intégrante du processus de déclaration à la CNIL des fichiers concernés, pour l'ensemble des unités concernées du CNRS.

3 - Les informations enregistrées

3.1 - Informations journalisés par les serveurs (hors messagerie et Web) et postes de travail

Pour chaque tentative de connexion ou d'ouverture de session de travail les informations suivantes - ou une partie de ces informations - peuvent être enregistrées automatiquement par les mécanismes de journalisation du service :

- L'identité de l'émetteur de la requête qui peut être :
  - dans le cas d'une authentification à l'aide d'un certificat les différents éléments de celui-ci : l'émetteur, le nom de l'utilisateur, son adresse électronique, le numéro de l'unité.
  - sinon on enregistre l'identifiant ou/et l'adresse IP (adresse proprement dite ou nom de machine et dans un certains nombre de cas le serveur DHCP, PXE).
  - On peut enregistrer aussi l'adresse Ethernet ou des informations identifiant la machine comme le nom que lui a donné son propriétaire ou même des identifiants internes ;
- La date et l'heure de la tentative ;
- Le résultat de la tentative (succès ou échec) ;
- Nombre de connexions ;
- Les commandes passées.

Le choix d'une politique de centralisation des traces des postes de travail peut être fait. Dans ce cas des événements comme la détection de virus, les différents mises à jour effectuées, les actions prises par le pare-feu individuel, etc. sont intéressants à remonter.

Ces données sont conservées au maximum pour une durée d'un an.

3.2 - Serveurs de messagerie (SMTP)

Les serveurs de messagerie enregistrent pour chaque message émis ou reçu les informations suivantes (ou une partie seulement de ces informations) :

- L’adresse de l’expéditeur et éventuellement des éléments identifiant celui qui s'est connecté au serveur SMTP lorsque est utilisé une authentification par identifiant/mot de passe ou par certificat. Par exemple pour éviter de laisser un relais ouvert à tout le monde mais faciliter la connexion des utilisateurs distants, il arrive de n’autoriser le relais qu'aux utilisateurs dûment authentifiés par certificat ;
- L’adresse du destinataire ;
- La date et l’heure de la tentative ;
- Les différentes machines (relais de messagerie) dont il est reçu des messages ou auxquelles il en est envoyé ;
- Le traitement « accepté ou rejeté » du message (on peut rejeter des messages ne respectant pas les standards) ;
- Le sujet du message dans le cas où il ne contiendrait pas que des caractères standards ;
- Parfois la taille du message ainsi que l'en-tête "message-id" qui peut contenir, en fonction des outils utilisés, des éléments formés à partir d'adresse électronique ;
- Le cas échéant le résultat du traitement antispam ou antivirus sur ce message.

Ces données sont conservées au maximum pour une durée d’un an.

Un contrôle antivirus sur les pièces jointes ou/et un filtrage de celle-ci en fonction de leur extension est systématiquement effectué sur les messages en entrée dans certaines unités du CNRS. En cas de détection de virus, le message peut être bloqué. Il est souhaitable que l’émetteur ou le destinataire en soit averti. Les messages infectés sont conservés quelques jours. Si l’utilisateur souhaite les conserver lui-même, il peut demander à les faire transférer, quand cela est possible, sur son poste de travail après désinfection.

Un plan de crise permettant d’assurer la continuité du service de messagerie peut prévoir le rejet systématique et sans « réponse automatique » des messages identifiés comme provenant d’un ver de messagerie. Le personnel doit alors être informé de l’existence de ce plan et le conseil de laboratoire avoir donné son accord sur la procédure suivie. Les utilisateurs doivent être prévenus lorsque le plan de crise est déclenché.

Les messages sont mis à la disposition des destinataires via des serveurs de messagerie. Le fait de laisser les messages sur le serveur ou de les rapatrier sur son poste relève de la responsabilité de chaque utilisateur. Seuls les administrateurs des serveurs ont la possibilité d’accéder, dans les limites de ce qui est nécessaire à l'accomplissement de leurs missions définies au paragraphe 7.2, aux informations stockées sur les serveurs qu’ils administrent.

Les traces des échanges sont conservées pour une durée d’un an maximum.

3.3 - Serveurs Web (HTTP)

Pour chaque connexion les serveurs Web enregistrent les informations suivantes (ou une partie seulement de ces informations) :

- L’adresse IP source et destination et les différentes données d'authentification (identifiant/authentifiant ou certificat) dans le cas où il est effectué une authentification de l'utilisateur ;

- La page consultée et les informations fournies par le client (navigateur, robot, ...) comme le type de navigateur et le système d'exploitation du client ;
- Les numéros des ports source et destination ainsi que le protocole ;
- Le type de la requête ;
- La date et l'heure de la tentative ;
- Le volume de données transférées ;
- Les différents paramètres passés au « cgi-bin » ;

Ces données sont conservées au maximum pour une durée d'un an.

3.4 - Les équipements d'extrémité de réseau et la surveillance des services réseau (routeurs, pare-feux, commutateur, borne d'accès, …)

Pour chaque paquet qui traverse l'équipement les informations suivantes (ou une partie seulement de ces informations) sont collectées :

- L'adresse IP source et destination ;
- Les numéros de port source et destination ainsi que le protocole. Ces informations permettent de déterminer le service demandé.
- La date et l'heure de la tentative ;
- La façon dont le paquet a été traité par l'équipement : transmis ou filtré.
- Le nombre de paquets et le nombre d'octet transférés pour chaque connexion (une connexion étant identifiée par la même adresse IP source, la même adresse IP destination, le même port source et le même port destination.)

S'ajoute, éventuellement, à ces informations pour certains types de matériel (pare-feux, sans fil utilisant les protocoles 802.1X dont l'authentification est indispensable.) les données d'authentification (identifiant ou certificat) et parfois l'historique des commandes passées.

Toutes ces données peuvent être conservées au maximum pour une durée d'un an.

3.5 - Système de détection d'intrusion (IDS) et de l'enregistrement des paramètres d'utilisations des services réseau.

Les IDS à détection par scénario ont pour rôle la remontée d'alerte en temps réel par la détection de signatures connues d'attaque. Les informations collectées par ces systèmes qui peuvent être l'ensemble des trames qui circulent sur le réseau ne sont stockées que le temps nécessaire à la remontée de l'alerte, sauf pour certaines unités de services utilisant des réseaux haut-débits sur lesquels il n'est pas possible, pour des raisons de performance, de faire fonctionner un IDS en temps réel. Dans ces cas exceptionnels, les traces peuvent être conservées le temps de les faire vérifier par un IDS hors connexion.

Les IDS à détection par comportement ne rentrent pas dans le cadre de ce document et doivent, quant à eux, faire l'objet d'une demande spécifique à la CNIL.

Les messages d'alerte des IDS sont quant à eux conservés pour une durée maximale d'un an.

3.6 - Les applications spécifiques.

On entend par "applications spécifiques", toute application autre que celles mentionnées ci-dessus qui nécessite pour des raisons de comptabilité, de gestion, de sécurité ou de développement, l'enregistrement de certains paramètres de connexion et d'utilisation. Il en est ainsi, par exemple, pour les SGBD (dont la sécurité sera renforcée quand ils traitent de données nominatives), les logiciels commerciaux partagés, les autres services réseau (FTP, SSH, …), l'instrumentation scientifique (pilotage d'appareillages ou de machines.), ou encore les applications à accès restreints comme celles relatives aux activités de gestion et de direction des laboratoires, des délégations régionales ou de l'organisme. Les informations suivantes (ou une partie seulement de ces informations) peuvent être collectées :

- Le n° IP source et l'identité de l'émetteur de la requête qui peut être :
    - dans le cas d'une authentification à l'aide d'un certificat les différents éléments de celui-ci.
    - sinon l'identifiant/authentifiant ou/et l'adresse IP (adresse proprement dite ou nom de machine et dans un certains nombre de cas le serveur DHCP, PXE).
    - on peut enregistrer aussi l'adresse Ethernet ou des informations identifiant la machine comme le nom que lui a donné son propriétaire ou même des identifiants internes ;
- La date et l'heure de la tentative ;
- Le résultat de la tentative (succès ou échec) ;
- Volumes de données transférées ;
- Nombre de connexions.

De plus, pour certaines applications, les traces peuvent comporter une fraction, ou un échantillon des données échangées. Cela peut être aussi le cas sans qu'il y ait nécessairement à une préoccupation de sécurité. En particulier, dans la mise au point de logiciel ou de réglage de paramètres, il est très souvent nécessaire d'activer un « mode bavard » pour retrouver les sources de dysfonctionnements éventuels. Un maximum d'informations sont alors temporairement enregistrées. Les utilisateurs doivent être avertis quand ce mode d'exploitation est activé.

Exception faite des traces de mise au point qui ne doivent être conservées que le temps nécessaire à rendre l'application stable, ces traces peuvent être conservées pour une durée maximum d'un an.

4 Les traitements effectués

Le triple objectif de ces traitements est de veiller :

- au respect de la politique de sécurité[2] ;
- au bon fonctionnement du matériel et logiciel ;

[2] La SSI est veiller au respect de la "politique de sécurité" clairement énoncé. Tant qu'il n'y a pas eu violation de la politique de sécurité, il n'y a pas eu incident de sécurité !

- à l’équilibrage de charge des équipements et logiciels.

Pour tout traitement répondant à d’autres objectifs que ceux-là, une demande d’autorisation spécifique devra être faite à la CNIL..

Les fichiers de traces contiennent un ensemble d'informations, relatives aux actions ou aux transactions accomplies, qui peuvent avoir un caractère nominatif par l’enregistrement du « login » ou de l’adresse IP d’une machine à partir desquels, par association, on peut identifier un utilisateur. Les traitements effectués sur ces informations doivent permettre d'obtenir des journaux qui répondent aux principes de base énoncés précédemment, tout en restant conformes aux obligations légales sur la protection des informations personnelles, en particulier celles concernant le respect de la vie privée et le principe d’information préalable et de transparence. Les traitements permettent d'obtenir :

- des résultats statistiques systématiques ;
- des résultats d'analyse ;
- des résultats ciblés et nominatifs ;
- des journaux bruts.

4.1- Des résultats statistiques systématiques

Ceux-ci, effectués automatiquement, permettent de contrôler les volumes d'utilisation des moyens mis à la disposition des utilisateurs en temps qu'outil de travail. Parmi ces traitements on trouvera : des traitements statistiques en anonymes en volume transféré et en nombre de connexions, des calculs de « top ten » des services les plus utilisés en volume de données et en nombre de connexion, des « top ten » des machines ayant consommé le plus de réseau en volume transféré et en nombre de connexions.

4.2 - Des résultats d'analyse

La vérification visuelle des traces ou le contrôle effectué manuellement d’événements atypiques permettent de veiller à l'application des règles de sécurité.

4.3 - Des résultats ciblés et nominatifs

Ceux-ci, sont effectués à la demande de l'utilisateur concerné lorsqu’il a cru déceler des actions anormales sur sa machine, ses fichiers ou ses applications.

4.4 - Des journaux bruts

Ceux-ci permettent de replacer une action particulière dans son contexte, à des fins d'enquête.

La production de journaux bruts sera requise dès l'apparition d'un incident. On considère comme incident tout événement ou comportement individuel non conforme aux politiques de sécurité ou aux règles d'exploitation en vigueur sur le système concerné.

Les administrateurs systèmes des unités du CNRS sont chargés de ces traitements. Ils sont, pour cette activité, soumis au secret professionnel.

5 - destinataires des traitements effectués

5.1 Destinataires des traitements statistiques

Des traitements systématiques sont effectués pour la métrologie générale des systèmes sur l'ensemble des données que constituent toutes les traces,. Il s'agit de traitements statistiques en volume et en nombre de connexions qui sont anonymes.

Ces traitements sont effectués de façon automatique et peuvent être diffusés sur des sites Internet accessibles à tous.

Les traitements statistiques de type « top ten » par service réseau ou par machine pouvant faire apparaître des adresses IP de machine personnelle permettant de remonter au nom de la personne en possession de cette machine, sont à la seule disposition des administrateurs système et réseau.

5.2 - Destinataires des analyses effectuées manuellement par les administrateurs système et réseau

La politique de sécurité, applicable à chaque moyen ou système qui génère des traces, définit des règles d'analyse systématique de ces traces afin de pouvoir détecter, dans les meilleurs délais, les incidents relatifs à la sécurité des systèmes d'information.

En cas d'incident ou de suspicion d'incident des analyses peuvent être faites sur les traces disponibles. Ces analyses sont faites par les administrateurs et les résultats sont transmis en cas de suspicions légitimes au directeur de l'unité, au CERT-Renater, aux coordinateurs sécurité régionaux et nationaux ainsi qu'au service du Fonctionnaire de sécurité défense en vue d'un éventuel dépôt de plainte.

Dans ce cas, l'accès aux trafics et aux traces est limité aux exploitants des systèmes en charge d'analyser l'incident. L'extraction de l'information et son utilisation sont strictement limitées à la résolution. Si l'incident n'est pas avéré les résultats d'analyse sont immédiatement détruits.

A ce stade les informations ayant un caractère nominatif et susceptibles notamment de mettre en cause des personnes identifiées demeurent confidentielles au niveau de l'administrateur système et réseau et ne sont pas transmises.

5.3 – Destinataires des journaux bruts

Les journaux bruts sont remis, sur requête, à l'autorité judiciaire afin de lui permettre de poursuivre une enquête.

5.4 - Les accès individuels

Chaque agent peut demander à consulter les traces télématiques ou informatiques qui le concernent. Les demandes doivent être faites par écrit auprès du directeur de l'unité concernée.

La recherche est faite par l'administrateur, sur demande de sa hiérarchie, et les résultats sont transmis directement à l'utilisateur demandeur, sous la forme d'un "courrier personnel".

6 - Informations des utilisateurs sur la politique de gestion des traces

Chaque unité doit informer les utilisateurs des moyens informatiques du laboratoire de la gestion qui est faite des traces qui les concernent. Cela sera fait par la diffusion systématique de la politique de gestion des traces (ce document) suivant le même protocole que pour la diffusion la charte informatique.

7- Les intervenants

7.1 - Les utilisateurs

Ils ont des droits. L'activité des utilisateurs génère des traces qui ne doivent pas subir des détournements de finalité. Ils ont des devoirs, dont l'essentiel est qu'ils sont responsables de l'utilisation des moyens mis à leur disposition, en temps qu'outils de travail, par le CNRS et qu'ils doivent respecter les règles d'utilisation et de sécurité définies dans la « **charte d'utilisation des moyens informatiques** » et **la politique de sécurité** définie par l'unité.

À ce titre, ils doivent formellement donner acte, par la signature d'une déclaration d'engagement du fait qu'ils ont été informés :

- De leur responsabilité de respecter les lois et les règlements ;
- Des règles de sécurité appliquées ;
- Des moyens mis en œuvre pour vérifier la bonne application de ces règles de sécurité et notamment le dispositif de gestion des traces ;
- Des règles et procédures liées à l'exploitation de ces moyens.

Il appartient à chaque agent titulaire de ces moyens de mettre en place ou de demander la mise en place des moyens de protection de manière à éviter toute utilisation abusive à son insu.

Ces moyens sont réservés à un usage professionnel dans le respect des règles de sécurité en vigueur. Même si une certaine tolérance peut être admise pour une utilisation personnelle ponctuelle, toute utilisation abusive voire délictueuse des moyens de communication entraîne la responsabilité personnelle et pénale de l'agent.

L'utilisateur est responsable de la protection de la confidentialité et de l'intégrité des informations auxquelles il peut avoir accès dans le cadre de son activité. À ce titre il devra s'interdire d'utiliser des moyens de transmissions télématiques qui ne sont pas conformes au niveau de sécurité nécessaire à la protection de ces informations.

7.2 - Les administrateurs système et réseau

Ils sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau et responsables du respect des règles de sécurité. À ce titre, ils gèrent les traces.

À ce titre, ils sont responsables de leur propre conduite et ils doivent formellement donner acte, par la signature d'une déclaration d'engagement du fait qu'ils ont été informés :

- De leur responsabilité de respecter les lois et les règlements ;
- De leur responsabilité du contrôle des règles de sécurité appliquées ;
- Des moyens dont ils disposent pour vérifier la bonne application de ces règles de sécurité ;
- Des règles et procédures liées à l'exploitation de ces moyens.

Ils rapportent toute anomalie de fonctionnement ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur le système ou les réseaux.

Ils acceptent d'exécuter des traitements ou de fournirent des informations pouvant inclure des données nominatives uniquement à la demande de la structure fonctionnelle de sécurité (fonctionnaire de sécurité de défense, coordinateurs sécurité), ceux-ci n'ayant pas de liens hiérarchiques directs et étant tenus comme eux au secret professionnel. Ils sont tenus à la discrétion la plus absolue et ne répondent, sauf réquisition de l'autorité judiciaire, à aucune autre demande d'information ou de traitement pouvant mettre en cause des personnes ou porter atteinte à leur vie privée.

7.3 - Le responsable de l'unité

Il représente l'unité du CNRS qu'il dirige. Sa responsabilité peut être engagée, dans la limite de ce qu'il peut connaître et de ce qu'il peut exiger, en cas d'incident ou d'accident impliquant l'unité dont il a la charge. Il s'assure de la diffusion de la charte d'utilisation des moyens informatiques auprès de chaque utilisateur et veille à son respect ainsi qu'à celui du règlement intérieur. Il n'a pas à avoir accès aux traces permettant de mettre en cause une personne.

7.4 - Les coordinateurs sécurité

Ils sont les interlocuteurs au quotidien des administrateurs pour la gestion et le contrôle des systèmes et des réseaux dans le respect des règles SSI.

Ils ont accès aux rapports d'analyse des traces des moyens et des systèmes mis en œuvre sur l'établissement. Ils ont en particulier accès aux informations nominatives et sont par

conséquent soumis au secret professionnel.

En cas d'incident de sécurité nécessitant une investigation, ainsi qu'en cas d'enquêtes internes ou diligentées par les autorités compétentes il rapporte tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur le système ou les réseaux.

7.5 - Le Fonctionnaire de Sécurité de Défense

Il est responsable, pour le CNRS, de l'application des lois et de la réglementation, en matière de sécurité et de protection de l'information. Il assure l'interface avec le Haut Fonctionnaire de Défense pour les questions de sécurité et de protection de l'information.

Il est responsable de la définition de la politique de sécurité des systèmes d'information et des réseaux pour le CNRS et de sa mise en œuvre dans les établissements.

Le Fonctionnaire de Sécurité de Défense est tenu informé par l'administrateur système local des incidents de sécurité touchant des systèmes d'information lorsque la gravité (constatée ou potentielle) de l'incident est susceptible d'avoir des suites juridiques (éventualité de dépôts de plainte, mise en cause de personnels dans le cadre d'analyses de traces...). En position fonctionnelle hors hiérarchie et tenu au secret professionnel, le FSD, après avis du directeur de l'unité, peut avoir accès à l'ensemble des informations relatives à ces incidents, y compris les journaux bruts des traces des systèmes concernés.

Dans le cadre des audits et contrôles de sécurité informatique qu'il est amené à conduire, il peut, sur motif sérieux touchant à la sécurité informatique de l'unité, et après avis du directeur de l'unité, demander de faire procéder à une enquête interne comportant une analyse nominative de traces.

7.6 – Le correspondant du CNRS auprès de la CNIL

Le CNRS a mis en place un correspondant auprès de la CNIL :

Madame Florence CELEN
UPS837, Direction des systèmes d'information (DSI)
TOUR GAIA
RUE PIERRE-GILLES DE GENNES
BP 193
31676 LABEGE CEDEX

Téléphone : 05 62 24 25 19
Adresse électronique : mailto:florence.celen@dsi.cnrs.fr