

**Politique de gestion**

des traces informatiques



“Des savoirs & des talents”

# Statut du document

Ce document est une adaptation, pour l'Université de Poitiers, de travaux réalisés, à partir de 2008, dans le cadre du groupe de travail SDS-SUP (Schéma Directeur de la Sécurité pour le SUPérieur), mandaté par la Conférence des Présidents d'Université (CPU), la Direction Générale de la Recherche et de l'Innovation (DGRI), la Direction Générale de l'Enseignement Supérieur (DGES) et le Haut Fonctionnaire de Défense et de Sécurité (HFDS) du ministère en charge de l'enseignement supérieur et la recherche.

La mission du groupe de travail SDS-SUP, animé par le CRU (Comité Réseau des Universités), était de mener des réflexions et de constituer un référentiel documentaire dans le domaine de la sécurité des systèmes d'information, notamment concernant les meilleures pratiques.

Le document « Politique type de gestion des journaux informatiques » a été élaboré en s'inspirant du document de « Politique de gestion des traces d'utilisation des moyens informatiques et des services réseau » du CNRS. Il a été mis à jour et complété afin de garantir la cohérence globale des référentiels et la conformité à la législation et aux réglementations en vigueur, notamment pour les points relevant de la loi « Informatique & Libertés ». Le partenariat CPU/CNIL a permis de mener un travail collaboratif conforme aux préconisations de la CNIL.

Ce document s'appuie aussi sur les productions suivantes :

- Note technique DAT-NT-012/ANSSI/SDE/NP « *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation* », Agence Nationale de la Sécurité des Systèmes d'Information, 2 déc. 2013
- *Livre blanc sur les logs*, Observatoire de la Sécurité des Systèmes d'Information et des Réseaux (OSSIR), 6 nov. 2009

Ce document est référencé dans la « *Charte d'utilisation des systèmes d'information* » de l'Université de Poitiers.

## Personnes ayant contribué à la rédaction de ce document

Rédacteurs	Contributeurs
Isabelle GUÉRINEAU <i>Correspondante Informatique &amp; Libertés (CIL)</i>	Éric ALVINERIE <i>Chargé de projets, DSI i-médias</i>
Emmanuel LAIZÉ <i>Responsable de la Sécurité des Systèmes d'Information (RSSI)</i> <i>Directeur adjoint des Systèmes d'Information (DSI adjoint)</i>	Emmanuel AUBIN <i>Vice-président Relations sociales, Affaires juridiques et éthique</i>
	Jean-François CERISIER <i>Vice-président Numérique et système d'information</i>
	Nirmal NIVERT <i>Directeur des Affaires Juridiques (DAJ)</i>
	Christophe QUINTARD <i>Directeur des Systèmes d'Information (DSI)</i>

## Évolutions du document

Version	Date	Nature des modifications
1.0	27 janvier 2017	Version initiale présentée au conseil d'administration du 27 jan. 2017

# Politique de gestion des traces informatiques à l'Université de Poitiers

---

## 1 Définitions

---

- on entend par « établissement », l'Université de Poitiers ;
- on entend par « utilisateur », toute personne, quel que soit son statut, ayant accès, dans le cadre de l'exercice de ses activités, aux ressources et moyens des systèmes d'information de l'établissement :
  - tout agent titulaire ou non titulaire, vacataire, stagiaire, hébergé, invité...
  - tout étudiant, en formation initiale, continue, présentielle ou à distance...
  - tout visiteur, participant aux colloques et événements organisés au sein de l'établissement...
  - etc.
- on entend par « systèmes d'information », l'ensemble des ressources et moyens informatiques (matériels, logiciels, applications, bases de données, ressources documentaires...) et moyens de communication électronique (réseaux de télécommunications, téléphones...) pouvant être mis à disposition de l'utilisateur, qu'ils soient accessibles dans les locaux de l'établissement ou à distance, directement ou en cascade à partir d'un réseau ;
- on entend par « entités », les facultés, instituts, écoles, laboratoires, services... de l'établissement.

## 2 Contexte

---

Le fonctionnement de l'établissement passe par l'utilisation de systèmes d'information s'appuyant sur des réseaux de communication connectés à l'échelle mondiale. Ces réseaux, qui apportent une souplesse inégalée, ont également une grande vulnérabilité intrinsèque. Leur utilisation engage la responsabilité personnelle des utilisateurs, ainsi que, dans certaines situations, celle de l'établissement qui les met à leur disposition en tant qu'outils de travail.

L'utilisation de ces technologies pose le problème de la protection, d'une part, de l'information sensible<sup>1</sup> gérée par les utilisateurs et, d'autre part, des systèmes d'information et de communication sous la responsabilité de l'établissement. Les mesures mises en œuvre doivent permettre à l'établissement de remplir ses missions tout en satisfaisant aux exigences qui sont imposées par ses engagements vis-à-vis de ses partenaires, des réglementations sur la protection des données sensibles, du patrimoine scientifique, des données à caractère personnel ainsi que de la sécurité des systèmes d'information.

Une déontologie et un contrôle de l'utilisation sont donc nécessaires, de même qu'une information et une sensibilisation des utilisateurs. L'établissement a mis en place des dispositions et moyens pour assurer la sécurité et le contrôle de l'utilisation des moyens de communication, et fixé les conditions d'utilisation de ces moyens, afin de garantir les droits individuels de chaque utilisateur ([4]).

## 3 Principes de base

---

La maîtrise du fonctionnement des systèmes d'information (fiabilité, sécurité), et la garantie de la légalité 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 journaux informatiques ou journaux de traces (*logs* en anglais).

Ces journaux et leur traitement doivent respecter les droits de chacun et notamment être conformes à la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 dite loi « Informatique & Libertés ». Ils doivent satisfaire au principe d'information et de transparence, ainsi qu'au régime déclaratif en vigueur auprès de la CNIL, en l'occurrence, pour la politique de gestion des traces informatiques à l'Université de Poitiers, une inscription au registre des traitements Informatique & Libertés par le CIL<sup>2</sup> de l'établissement.

---

<sup>1</sup> « information sensible » au sens où la confidentialité (contrat, donnée de recherche, information nominative...), l'intégrité (information de gestion...) et la disponibilité nécessitent une protection particulière.

<sup>2</sup> Le Correspondant Informatique & Libertés (CIL) a un rôle de conseil et de suivi dans la légalité de déploiement des projets numériques de l'établissement et, plus largement, de la gestion des données à caractère personnel. Il consigne, au sein du registre des traitements Informatique & Libertés, les traitements ordinaires et courants ; seuls ceux identifiés comme sensibles dans la loi demeurent soumis à autorisation de la CNIL.

### 3.1 Finalités des traitements de journaux de traces

Les traitements des journaux de traces ont pour finalités de :

- contrôler le volume d'utilisation des ressources, détecter des anomalies afin de mettre en place une qualité de service et faire évoluer les équipements en fonction des besoins (métrologie) ;
- vérifier que les règles en matière de sécurité des systèmes d'information sont correctement appliquées ;
- 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 de l'établissement ;
- détecter les utilisations des moyens informatiques contraires aux chartes ou au règlement intérieur de l'établissement ;
- être à même de fournir des éléments de preuves nécessaires pour mener les enquêtes en cas d'incident et de répondre à toute réquisition de l'autorité judiciaire présentée dans les formes légales.

Les finalités précitées imposent d'aller au-delà d'une simple consignation et d'une exploitation de données statistiques. Elles impliquent nécessairement l'enregistrement, la conservation temporaire et l'éventuelle exploitation de données à caractère personnel, dans la mesure où des éléments contenus dans les traces permettraient de remonter à l'utilisateur.

### 3.2 Durée de conservation

La durée de conservation des journaux de traces est de 1 an maximum<sup>3</sup>. L'établissement s'interdit de les exploiter au-delà de 3 mois (cf. article 6), sauf sur réquisition officielle. Une politique de rotation des journaux de traces est mise en œuvre au sein du système de journalisation dans le but de garantir leur suppression automatique au-delà d'une année.

### 3.3 Qualités des données collectées

Les informations journalisées sont factuelles et contextuelles. Elles doivent permettre de connaître l'environnement de la collecte, le système hôte, les logiciels mis en œuvre... Chaque événement fait mention d'une source identifiable (équipement, utilisateur, processus...) permettant de déterminer avec le plus de précision possible son origine.

De même, un événement journalisé n'est pertinent que s'il est horodaté. L'heure relevée est une information importante parce qu'elle est souvent le premier élément utilisé pour rapprocher des journaux de différents systèmes. Il est donc indispensable que les équipements produisant des traces soient synchronisés sur les mêmes sources de temps internes.

### 3.4 Sécurité et intégrité des données

La politique en matière de sécurité des systèmes d'information (SSI) fixe les règles de sécurité appliquées aux fichiers de journaux. Ces fichiers sont, en particulier, protégés contre un effacement ou des modifications malveillantes. Une base « d'empreintes numériques » permet de surveiller leur intégrité. Les traces sont transférées en temps réel sur une machine différente de celle qui les a générées.

Les accès aux fichiers de journaux sont limités aux seuls intervenants autorisés (cf. article 4), au travers d'un réseau privé et après authentification. Ces accès sont ponctuels et motivés par les tâches de ces personnes. Dans le cadre d'une requête légitime (cf. article 5), seuls les extraits concernés par la demande seront transmis, et ce, de manière sécurisée (chiffrement des données, remise en main propre...).

## 4 Intervenants

---

L'ensemble des intervenants sont tenus au devoir de réserve ou de discrétion professionnelle, voire au secret professionnel en fonction de leur mission.

### 4.1 La chaîne fonctionnelle SSI

- l'autorité qualifiée de sécurité des systèmes d'information (AQSSI),
- le fonctionnaire de sécurité de défense (FSD),
- le responsable de la sécurité des systèmes d'information (RSSI) et ses adjoints.

L'accès aux journaux de traces de plus de 3 mois est réservé aux acteurs de la chaîne fonctionnelle SSI, pour la mise en œuvre du droit d'accès aux intéressés et l'accès sur requête judiciaire.

<sup>3</sup> Cette durée s'appuie sur Art. 6.II de la loi n°2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique.

## 4.2 Les autres intervenants

Outre la gestion des journaux dans le respect des obligations générale de leur fonction, les acteurs définis ci-après acceptent d'exécuter des traitements ou de fournir des informations pouvant inclure des données à caractère personnel uniquement à la demande de la chaîne fonctionnelle SSI.

### 4.2.1 Les administrateurs systèmes et réseau

Les administrateurs systèmes et réseau sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau. Ils veillent au respect des règles de SSI, et rapportent au RSSI tout incident pouvant laisser supposer un problème de sécurité. On distingue :

- les administrateurs systèmes et réseau de la Direction des Systèmes d'Information (DSI *i*-médias), pour les systèmes d'information de l'établissement ;
- les correspondants informatiques, pour les systèmes d'information de gestion propres à leur entité.

### 4.2.2 Les gestionnaires d'équipements ou d'applicatifs métiers

Certains équipements ou applicatifs métiers permettent un accès restreint à leurs journaux de traces. On peut citer, pour l'établissement, le système de contrôle d'accès, et, pour les entités, certains matériels expérimentaux. Les gestionnaires de ces systèmes ne peuvent prendre connaissance de ces journaux qu'à des fins de gestion, détection d'anomalie, remontée d'alarmes techniques...

## 5 Destinataires et tiers autorisés

---

### 5.1 Les destinataires légitimes

Dans le cadre de la détection des usages abusifs (contraire aux lois, au règlement intérieur ou chartes de l'établissement), la Direction des Affaires Juridiques ou les membres des sections disciplinaires peuvent, de manière légitime, recevoir ponctuellement communication d'extraits des journaux de traces.

Dans le cadre de l'analyse d'incidents de sécurité, les services du centre d'alerte et de réaction aux attaques informatiques de Renater (CERT-Renater) et de l'Agence Nationale de la Sécurité des Systèmes d'Information (CERT-FR) sont inscrits en tant que destinataires légitimes.

### 5.2 Les tiers autorisés

La loi permet à des autorités publiques de se faire communiquer, dans le cadre de leurs missions et, sous certaines conditions<sup>4</sup>, des informations issues des journaux de traces. La demande doit être ponctuelle et préciser par écrit le texte législatif fondant ce droit de communication.

## 6 Traitements effectués

---

Les traitements effectués doivent répondre aux principes de base énoncés précédemment, tout en restant conformes aux obligations légales sur la protection des données à caractère personnel et de la vie privée. Quand ils sont mis en œuvre, ces traitements le sont de façon systématique, c'est-à-dire qu'ils ne ciblent aucune personne ou catégorie de personnes<sup>5</sup>.

### 6.1 Résultats statistiques

Des traitements permettant de contrôler les volumes d'utilisation des moyens mis à la disposition des utilisateurs en tant qu'outil de travail sont effectués automatiquement :

- détection des anomalies afin de mettre en place une qualité de service ;
- statistiques en volume transféré et en nombre de connexions ; classements des services les plus utilisés afin de faire évoluer les équipements en fonction des besoins.

Dans le cadre d'études statistiques nécessitant un historique, les fichiers de traces peuvent être rendus anonymes, au travers d'un processus irréversible réalisé sur une copie des journaux<sup>6</sup>. Les données résultantes peuvent être alors conservée et exploitée au-delà des délais mentionnés au paragraphe 3.2.

---

<sup>4</sup> Cf. [1], fiche pratique n°16 « Communication à des tiers autorisés d'informations relatives aux personnels et aux étudiants »

<sup>5</sup> Cf. [1], fiche pratique n°13 « Contrôle de l'utilisation des moyens informatiques »

<sup>6</sup> Dans le respect des règles de l'art publiées par la CNIL dans ce domaine  
<https://www.cnil.fr/fr/le-g29-publie-un-avis-sur-les-techniques-danonymisation-0>

## 6.2 Résultats d'analyse

La politique en matière de SSI, applicable à chaque ressource qui génère des traces informatiques, 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. Il faut garder à l'esprit que l'activité de journalisation est un moyen de détection et d'analyse : elle ne se substitue pas aux mécanismes de protection des systèmes d'information, elle doit être employée de façon complémentaire.

En cas d'incident ou anomalie de fonctionnement, des analyses peuvent être réalisées par les administrateurs systèmes et réseau sur les traces disponibles, en concertation avec le RSSI et/ou ses adjoints. L'extraction des informations et leur utilisation sont strictement limitées à l'analyse de l'incident. Les résultats ne peuvent être transmis qu'à la chaîne fonctionnelle SSI et, en cas d'incident de sécurité, au CERT-Renater et CERT-FR. Si l'incident n'est pas avéré, les résultats sont alors immédiatement détruits.

## 6.3 Détection des usages abusifs

On entend ici par « usages abusifs », les usages du réseau qui sont contraires aux lois, règlement intérieur ou chartes de l'établissement. Sont aussi visés les usages qui compromettent les services du réseau de l'établissement (consommation excessive de bande passante, introduction de vulnérabilités...).

Les journaux de traces peuvent être exploités pour mettre en évidence ces abus. Par exemple, le classement des machines ayant consommé le plus de réseau – en volume transféré et en nombre de connexions – permet souvent de détecter le partage de fichiers en violation du droit d'auteur via des systèmes pair à pair (*peer to peer* en anglais), ou la présence de serveurs pirates.

## 6.4 Requête émise par un tiers autorisé

L'analyse des journaux de traces d'un ensemble de composants (postes de travail, équipements réseaux, serveurs...), permet de replacer une action particulière dans son contexte, en particulier, à des fins d'enquête. La chaîne fonctionnelle SSI est en charge de la gestion des réquisitions émises par un tiers autorisé. Elle doit s'assurer de la légitimité de la demande : conformité aux textes invoqués dans la requête, vérification de l'identité et de la qualité du demandeur...

Les administrateurs systèmes et réseau, en concertation avec le RSSI et/ou ses adjoints, sont chargés de l'application de la requête ; ils sont, pour cette activité, soumis au secret professionnel. Les extraits de journaux de traces concernés par la requête, et les éventuelles analyses associées, sont remis en main propre au tiers demandeur afin de lui permettre de poursuivre son enquête. Ces éléments sont consignés dans un registre par le RSSI.

## 6.5 Droit d'accès individuel

Chaque utilisateur peut demander à consulter les traces qui le concernent. Les demandes doivent être faites par écrit auprès du CIL de l'établissement. Conformément à l'article 39 de la loi Informatique & Libertés, et à l'article 92 du décret n°2005-1309<sup>7</sup>, les personnes souhaitant exercer leur droit d'accès doivent justifier de leur identité.

La recherche est faite par les administrateurs systèmes et réseau, sur demande du CIL de l'établissement, et les résultats sont transmis directement à l'utilisateur demandeur, sous la forme d'un courrier personnel.

# 7 Types d'informations collectées

---

Ce document n'a pas vocation à présenter la liste exhaustive des informations collectées, celles-ci étant dépendantes des systèmes et des applications en vigueur. Ces données sont détaillées sur le site web de la DSI *i*-médiat, et mises à jour en cas d'évolution des systèmes d'information (prise en compte des nouveaux équipements, des nouveaux usages...).

À fin d'information des utilisateurs, nous décrivons ci-après les informations enregistrées dans les principaux journaux de traces.

## 7.1 Informations journalisées par les serveurs et les postes de travail

Pour chaque tentative de connexion, d'ouverture de session de travail ou de demande d'élévation de privilèges sur les serveurs et les postes de travail, tout ou partie des informations suivantes peuvent être enregistrées automatiquement par leurs mécanismes de journalisation :

---

<sup>7</sup> Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi Informatique & Libertés

- la date et l'heure de l'événement ;
- le processus système, l'utilisateur... à l'origine de l'événement ;
- les commandes passées et leurs résultats (succès, échec).

Les journaux de traces des serveurs de l'établissement font l'objet d'une centralisation sur le système de journalisation de la DSI *i*-médiat.

## 7.2 Équipements réseau

On appelle équipements réseau, les matériels qui concourent au transport des données sur les réseaux de communication : commutateur, borne Wi-Fi, routeur, pare-feu, serveur mandataire (*proxy* en anglais), accès nomade VPN... Pour chaque « communication » qui traverse l'équipement, tout ou partie des informations suivantes peuvent être enregistrées :

- la date et l'heure de l'événement ;
- les adresses IP<sup>8</sup> source et destination de la communication ;
- les adresses matérielles source et destination des équipements impliqués dans la communication ;
- les numéros de port (identifiant le service accédé) source et destination de la communication ;
- le résultat du traitement de la communication et les éventuels messages d'alerte qui en découlent ;
- le volume des données qui ont transité ;
- la durée de la communication ;
- l'identification de la ressource concernée par la communication, quand cela s'applique ;
- les informations d'authentification, quand cela s'applique.

## 7.3 Services d'authentification

Afin de simplifier les mécanismes d'authentification pour les utilisateurs, l'établissement a mis en place un service centralisé pour les applications et services internes à l'établissement, et des services fédératifs / coopératifs pour l'accès aux ressources numériques externes ainsi que pour la connexion aux réseaux Wi-Fi des partenaires de l'établissement. Ces services enregistrent tout ou partie des informations suivantes :

- la date et l'heure de l'événement ;
- l'identité de l'utilisateur (identifiant, adresse électronique...) de la requête ;
- le résultat du traitement de l'authentification ;
- un numéro de ticket unique associé à toute authentification valide ;
- les services accédés suite à l'authentification.

## 7.4 Services de messagerie, de messagerie instantanée, de forum et de listes de diffusion

Les serveurs mettant en œuvre ces services enregistrent, pour chaque message émis ou reçu, tout ou partie des informations suivantes :

- la date et l'heure de l'événement ;
- l'adresse électronique et l'adresse IP de l'expéditeur, et son authentification lorsqu'elle est requise par le service d'envoi ;
- l'adresse électronique de chaque destinataire ;
- certains en-têtes spécifiques, tel que l'identifiant numérique unique du message ;
- le résultat des traitements du message pour la détection de virus, de courriers non sollicités (spam)... ;
- les opérations de validation ou de rejet par les modérateurs, quand cela s'applique.

Le protocole de messagerie retranscrit ces éléments de traces dans les en-têtes du message, et ce, pour l'ensemble des serveurs ayant participé à son acheminement (de l'émetteur au destinataire).

## 7.5 Services web

Les serveurs hébergeant les sites et plateformes web de l'établissement enregistrent, pour chaque demande d'accès à une page, une image, une vidéo..., tout ou partie des informations suivantes :

- la date et l'heure de l'événement ;
- l'adresse IP du demandeur ;
- l'adresse de la ressource (URL) consultée par le demandeur, et les éventuels paramètres passés ;
- l'adresse de la page de provenance si la consultation résulte d'un lien cliqué ;
- le type de la requête et le résultat de son traitement (succès, erreur...) ;
- les informations fournies par le navigateur web du demandeur ;
- le volume de données transférées ;
- les informations d'authentification, quand cela s'applique.

<sup>8</sup> La Cour de Cassation – Chambre civile 1, 03 nov. 2016, 15-22595 – ainsi que la Cour de Justice de l'Union Européenne – deuxième chambre, 19 oct. 2016 , C-582/14 – ont reconnu, à l'adresse IP, un statut de donnée à caractère personnel.

## 7.6 Téléphonie

Le régime déclaratif des journaux de traces de téléphonie fixe ou mobile est régi par la norme simplifiée NS-047<sup>9</sup> relative à la gestion de la téléphonie sur le lieu de travail. Les équipements mettant en œuvre les appels téléphoniques entrants et sortants enregistrent tout ou partie des informations suivantes :

- la date et l'heure de début de la communication ;
- la durée de la communication ;
- l'identification du poste (n° de ligne) recevant l'appel ou le composant ;
- le numéro composé ou reçu ;
- le service de téléphonie utilisé, quand cela s'applique.

Ces éléments sont notamment utilisés pour la maîtrise des dépenses de communication, et la refacturation des appels sortants aux entités<sup>10</sup>. Lorsque des relevés justificatifs des numéros de téléphone appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés. L'établissement peut cependant éditer l'intégralité des numéros appelés dans le cas où il constate une utilisation manifestement anormale au regard de l'utilisation moyenne des services de téléphonie au sein de l'établissement.

L'usage de la téléphonie sur IP, et des services qu'elle apporte, peut engendrer des enjeux spécifiques dans le domaine de la sécurité ou dans celui du contrôle du bon fonctionnement des réseaux. Les principes relatifs à la loi Informatique & Libertés s'appliquent à la téléphonie sur IP comme aux autres systèmes de téléphonie. Tout ou partie des informations suivantes pourront compléter les données listées ci-dessus :

- les adresses IP source et/ou destination de la communication ;
- les adresses matérielles source et/ou destination des équipements impliqués dans la communication ;
- les numéros de port (identifiant le service accédé) source et/ou destination de la communication ;
- les services utilisés ;
- ...

## 7.7 Applications spécifiques

On entend par « application spécifique », toute application, autre que celles mentionnées ci-dessus, qui nécessite pour des raisons de comptabilité, de gestion, de sécurité ou de développement, l'enregistrement d'informations de traces (connexion, utilisation...). On peut citer l'accès aux applications métiers (finances, gestion RH, gestion des enseignements et des étudiants), l'accès aux bases de données...

Des journaux spécifiques sont susceptibles d'être constitués et tout ou partie des informations suivantes peuvent être collectées :

- la date et l'heure de l'événement ;
- l'identité du demandeur ;
- le résultat du traitement de la demande ;
- les actions et commandes effectuées.

## 8 Références

---

- [1] *Guide "Informatique et Libertés" pour l'enseignement supérieur et la recherche* – CPU, AMUE, CNIL 2011  
Disponible sur [https://www.cnil.fr/sites/default/files/typo/document/Guide\\_AMUE\\_2011.pdf](https://www.cnil.fr/sites/default/files/typo/document/Guide_AMUE_2011.pdf)
- [2] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation* (note technique DAT-NT-012/ANSSI/SDE/NP) – ANSSI 2 déc. 2013.  
Disponible sur [https://www.ssi.gouv.fr/uploads/IMG/pdf/NP\\_Journalisation\\_NoteTech.pdf](https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Journalisation_NoteTech.pdf)
- [3] Livre blanc sur les logs – OSSIR 6 nov. 2009  
Disponible sur [http://www.ossir.org/uploads/media/OSSIR\\_Livre-blanc\\_Logs\\_v1.pdf](http://www.ossir.org/uploads/media/OSSIR_Livre-blanc_Logs_v1.pdf)
- [4] *Charte d'utilisation des systèmes d'information* – Université de Poitiers

---

<sup>9</sup> <https://www.cnil.fr/fr/declaration/ns-047-gestion-de-la-telephonie-sur-le-lieu-de-travail>

<sup>10</sup> Cf. [1], fiche pratique n°11 « Utilisation du téléphone sur le lieu de travail »

[www.univ-poitiers.fr](http://www.univ-poitiers.fr)



“Des savoirs & des talents”



Université  
de Poitiers