Recommandations sur la gestion des logs au CNRS

DRUILHET Frédéric

RSI et RSSI-Régional
Correspondant PPST et RGPD

Frederic.Druilhet@cnrs.fr

16/02/2023 - Capitoul

Plan

- Introduction
- Le site sécurité-SI
- La décision en vigueur au CNRS
- Règles EXP-5 ** de la PSSI-CNRS
- Règles EXP-7 *** de la PSSI
- Règles clientes
- Développement

Site sécurité-SI et décision en vigueur

Site sécurité-SI

https://securite-si.cnrs.fr/consignes/gestion-traces/

Retrouver l'auteur -> Imputabilité
Démontrer l'action -> Non-répudiation

Attention : pas d'autre finalité que …

La note DEC1233250DAJ

- Abroge la décision 04P014DSI du 11 octobre 2004 portant création des traitements informatiques pour l'enregistrement des traces (lien)

- Mise en œuvre dans l'ensemble des laboratoires
- Conservation 1 an
- Destinataires : chaine fonctionnelle SSI
- FSD et DU sont chargés de l'exécution

Décision n° 04P014DSI du 11 octobre 2004 portant création de traitements informatisés ayant pour objet la gestion des traces générées par l'utilisation des moyens informatiques et des services réseau au CNRS

Direction des systèmes d'information

Vu L. n° 78-17 du 06-01-1978 mod., not. art. 22 ; D. n° 78-774 du 17-07-1978 mod. ; D. n° 82-993 du 24-11-1982 mod. ; récépissé de la CNIL du 30-09-2004.

Art. 1er. - Des traitements automatisés de données à caractère personnel ayant pour objet la gestion des traces générées par l'utilisation des moyens télématiques et informatiques sont créés au Centre national de la recherche scientifique 1 (CNRS). Ces traitements sont mis en œuvre dans l'ensemble des laboratoires sous tutelle CNRS.

Art. 2. - Les catégories de données à caractère personnel enregistrées sont celles décrites dans le document « politique de gestion des traces d'utilisation des moyens informatiques et des services réseau au CNRS ».
Les données à caractère personnel sont conservées un an.

Art. 3. - Les destinataires et les catégories de destinataires de ces informations sont celles décrites dans le document « politique de gestion des traces d'utilisation des moyens informatiques et des services réseau au CNRS » :
– le fonctionnaire de sécurité de défense,
– les responsables d'unité,
– les coordinateurs sécurité,
– les administrateurs système.

Art. 4. - Le droit d'accès prévu par l'article 38 et suivants de la loi n° 78-17 du 6 janvier 1978 modifiée s'exerce auprès du responsable du traitement au sein de l'unité concernée.

Art. 5. - Le fonctionnaire de sécurité de défense et les directeurs d'unité sont chargés de l'exécution de la présente décision qui sera publiée au *Bulletin officiel* du Centre national de la recherche scientifique.

Fait à Paris, le 11 octobre 2004.

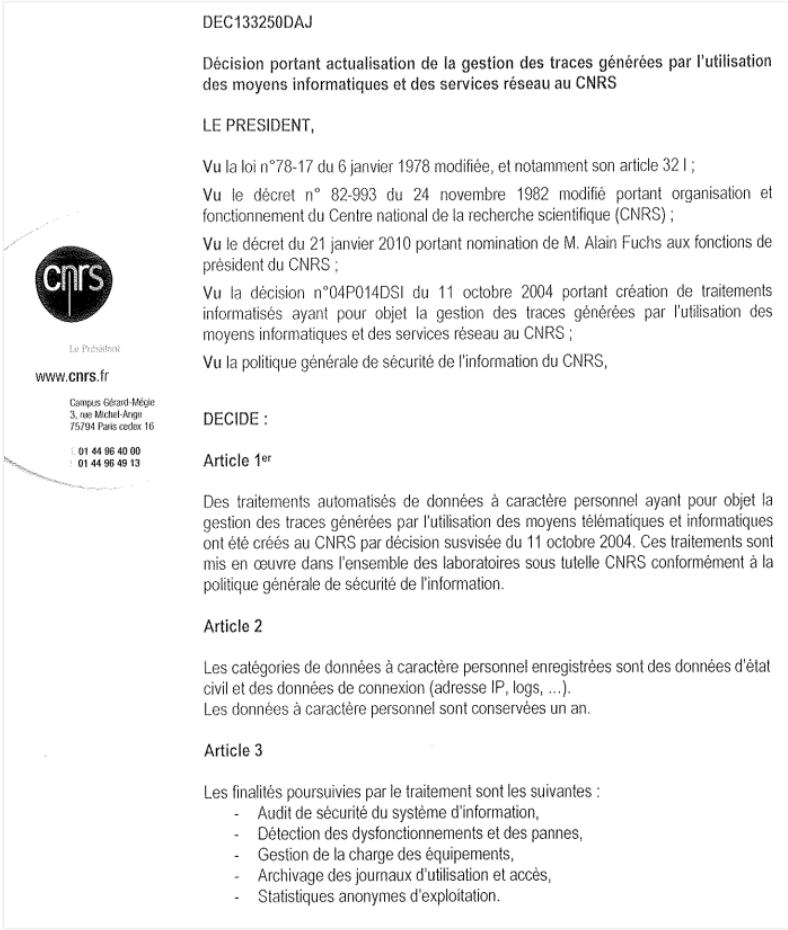
Pour le directeur général et par délégation :
Le secrétaire général,

Jacques BERNARD

1 Dont le siège est situé, 3, rue Michel Ange, 75794 Paris Cedex 16

La note DEC1233250DAJ

- **Note du PDG Alain Fuchs du 8 janvier 2014**
- **Finalités poursuivies traitement**
  - Audit de sécurité
  - Détection des dysfonctionnements et pannes
  - Gestion de la charge
  - Archivage des journaux
  - Statistiques anonymes
- **Destinataires**
  - ASR
  - Responsables unités
  - Chaine fonctionnelle SSI
  - Cert(s) et prestas techniques CNRS



cnrs

Le Président

www.cnrs.fr

Campus Gérard-Mégie
3, rue Michel-Ange
75794 Paris cedex 16

01 44 96 40 00
01 44 96 49 13

DEC133250DAJ

Décision portant actualisation de la gestion des traces générées par l'utilisation des moyens informatiques et des services réseau au CNRS

LE PRESIDENT,

Vu la loi n°78-17 du 6 janvier 1978 modifiée, et notamment son article 32 I ;

Vu le décret n° 82-993 du 24 novembre 1982 modifié portant organisation et fonctionnement du Centre national de la recherche scientifique (CNRS) ;

Vu le décret du 21 janvier 2010 portant nomination de M. Alain Fuchs aux fonctions de président du CNRS ;

Vu la décision n°04P014DSI du 11 octobre 2004 portant création de traitements informatisés ayant pour objet la gestion des traces générées par l'utilisation des moyens informatiques et des services réseau au CNRS ;

Vu la politique générale de sécurité de l'information du CNRS,

DECIDE :

Article 1er

Des traitements automatisés de données à caractère personnel ayant pour objet la gestion des traces générées par l'utilisation des moyens télématiques et informatiques ont été créés au CNRS par décision susvisée du 11 octobre 2004. Ces traitements sont mis en œuvre dans l'ensemble des laboratoires sous tutelle CNRS conformément à la politique générale de sécurité de l'information.

Article 2

Les catégories de données à caractère personnel enregistrées sont des données d'état civil et des données de connexion (adresse IP, logs, ...).
Les données à caractère personnel sont conservées un an.

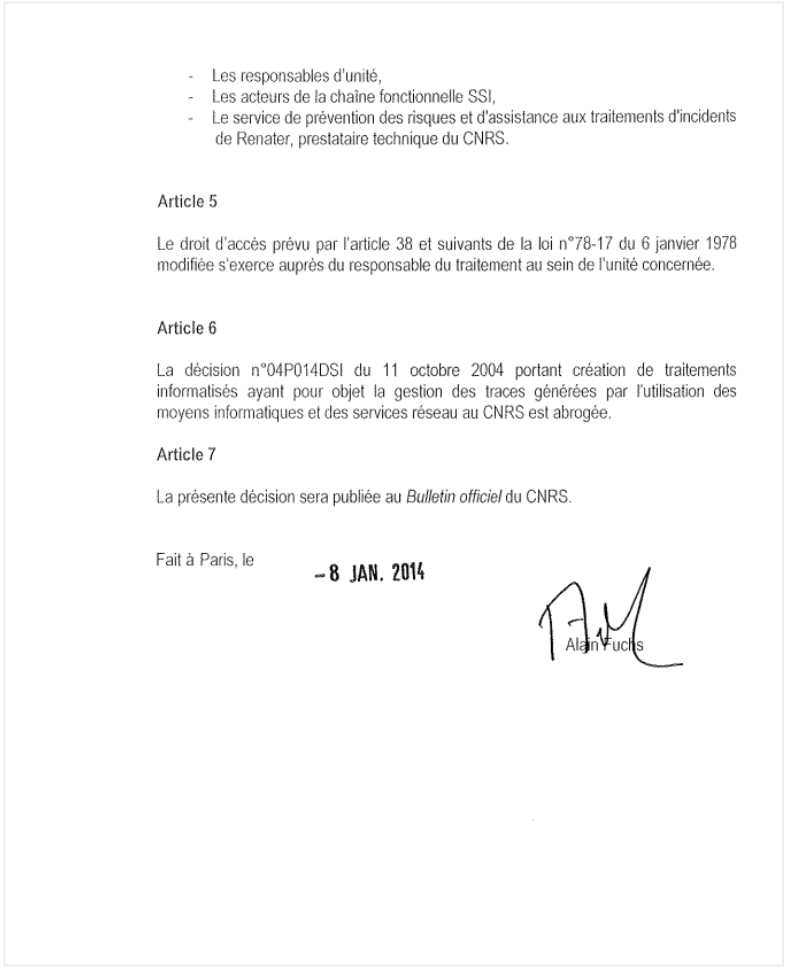
Article 3

Les finalités poursuivies par le traitement sont les suivantes :

- Audit de sécurité du système d'information,
- Détection des dysfonctionnements et des pannes,
- Gestion de la charge des équipements,
- Archivage des journaux d'utilisation et accès,
- Statistiques anonymes d'exploitation.

La note DEC1233250DAJ

- **La trace:**
  - un enregistrement unique généré par événement (connexion, déconnexion, action, erreur…)
  - la trace comporte un horodatage fiable (basé sur une source de temps elle-même fiable)
  - le format généré est exploitable facilement (on préférera toujours un format texte [csv, json…])
  - la trace comporte un identifiant de l'utilisateur/de son terminal, plusieurs si possible (nom,IP)
  - la trace porte le nom du système générateur (facilite le traitement lors de la centralisation)
- **Conservation**
  - La trace est complète
  - La trace est intègre
  - Sécurisée (protection, sauvegarde)
- **(lien)**



- Les responsables d'unité,
- Les acteurs de la chaîne fonctionnelle SSI,
- Le service de prévention des risques et d'assistance aux traitements d'incidents de Renater, prestataire technique du CNRS.

Article 5

Le droit d'accès prévu par l'article 38 et suivants de la loi n°78-17 du 6 janvier 1978 modifiée s'exerce auprès du responsable du traitement au sein de l'unité concernée.

Article 6

La décision n°04P014DSI du 11 octobre 2004 portant création de traitements informatisés ayant pour objet la gestion des traces générées par l'utilisation des moyens informatiques et des services réseau au CNRS est abrogée.

Article 7

La présente décision sera publiée au *Bulletin officiel* du CNRS.

Fait à Paris, le – 8 JAN. 2014

Alain Fuchs

Dans la PSSI CNRS

Quelques règles

Règle EXP-5* de la PSSI (lien)

- **Exploitation des SI: « *La gestion des traces de l'activité des systèmes informatiques doit respecter les directives nationales* » [(voir plus haut)]:**
  - **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.

Règle EXP-5* de la PSSI (lien)

- **Exemples de traces à collecter**
  - les serveurs et postes de travail ;
    - Serveurs de messagerie
    - Serveurs Web
    - Informations journalisés par les autres 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, ...) ;
  - tout équipement informatique fourni à l'utilisateur par le CNRS ou ses partenaires à des fins professionnelles ;
  - les applications spécifiques
    - SGBD
    - ftp, ssh, appareillage scientifique

Règle EXP-5* de la PSSI (lien)

- **Conservation (définie par EXP-5-1 **)**
  - Durée maximale 12 mois.
  - Si centralisation (préconisé): 1 mois et 12 sur le concentrateur
- **Ce dernier devient un élément sensible du SI (cf PDI-3 ** un peu plus loin)**
- **RGPD**
  - **finalité** : usage déterminé et légitime ;
  - **proportionnalité** : informations pertinentes et nécessaires ;
  - **durée limitée** de conservation des données ;
  - **sécurité et de confidentialité** : le responsable du traitement doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation ;
  - **respect du droit des personnes**.
- **Attention !! L'utilisateur doit en être informé via lecture de la charte SSI (lien)**

Règle EXP-7*** de la PSSI (lien)

- **Exploitation des SI: «** ***Les traces générées par les systèmes informatiques (serveurs, postes de travail, matériels actifs, etc.) sont régulièrement analysées pour détecter d'éventuels évènements anormaux.*** **» :**

- **Nécessite EXP-5* et EXP-5-1****
- **Outillage SIEM (Security Information and Event Management)**
  - Collecte
  - Normalisation
  - Agrégation
  - Corrélation
  - Alerte, reporting
  - Archivage
  - Analyse (rejeu)

Voir présentations suivantes

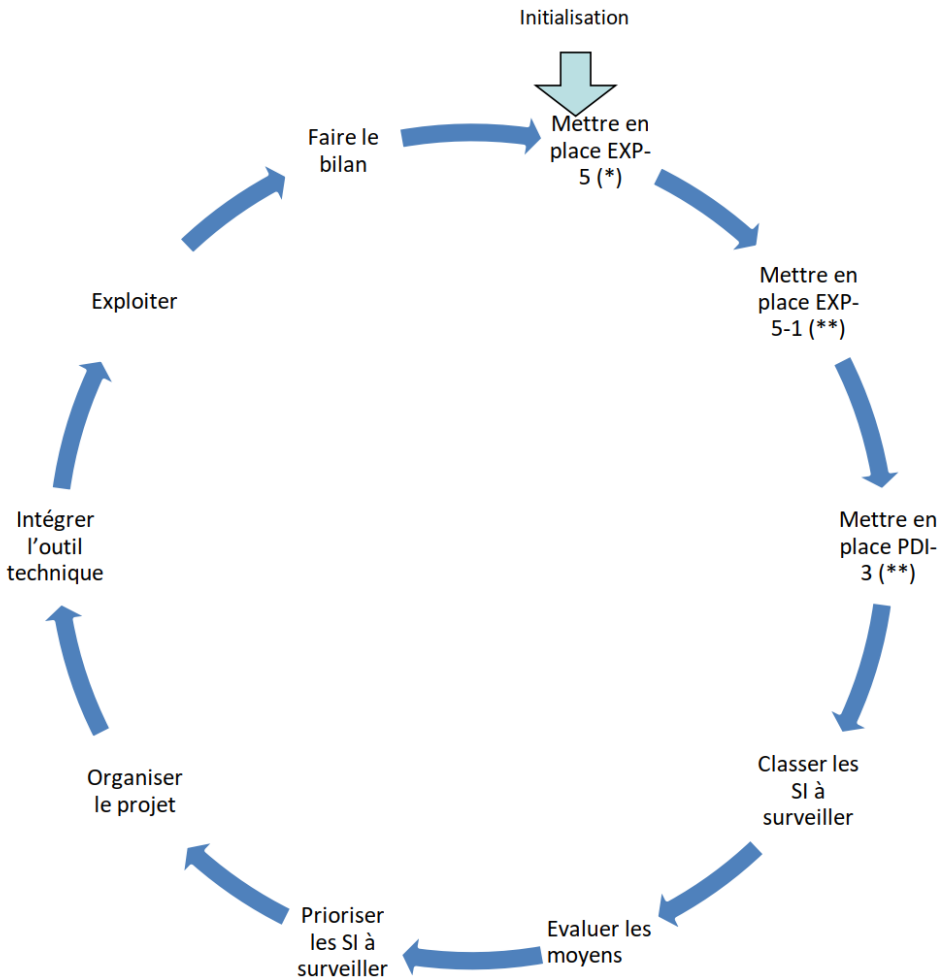
Règle EXP-7*** de la PSSI (lien)

- **Exploitation des SI: «** ***Les traces générées par les systèmes informatiques (serveurs, postes de travail, matériels actifs, etc.) sont régulièrement analysées pour détecter d'éventuels évènements anormaux.*** **» :**

- **Nécessite EXP-5* et EXP-5-1****
- **Outillage SIEM (Security Information and Event Management)**
  - Collecte
  - Normalisation
  - Agrégation
  - Corrélation
  - Alerte, reporting
  - Archivage
  - Analyse (rejeu)

Voir présentations suivantes

La démarche souhaitée



Autres règles de la PSSI

Autres règles de la PSSI

- **PDI-3 ** - Protection des documents et des informations**
  - Les systèmes d'information utilisés dans l'unité doivent être référencés et leur niveau de sensibilité évalué
  - https://securite-si.cnrs.fr/bonnes-pratiques/sensibilite/
- **AUTH-1 * - Authentification et contrôle d'accès**
- **PDI-6 ** - Protection des documents et des informations**
  - des traces à effacer ou éviter également !
  - Guide CNRS sur les traceurs de sites web (lien - mise à jour 07/12/2022)
- **PHY-2-1 *** et PHY-2-2 *** - Sécurité physique**
  - Traçabilité des accès physiques
  - Protection des accès physiques

Et on n’oublie pas:

- **Le développement !!**
  - Traces applicatives
    - Journalisation des accès
    - Journalisation des actions
    - Guide CNIL RGPD pour les développeurs
      https://lincnil.github.io/Guide-RGPD-du-developpeur/
- **Correspondance PSSI CNRS <--> PSSI-e**

AUTH-1 *	EXP-POL-ADMIN
EXP-5 *	EXP-JOUR-SUR, EXP-POL-JOUR, EXP-CONS-JOUR
EXP-7 ***	EXP-GES-DYN
EXP-5-1**	EXP-GEST-ADMIN, EXP-POL-JOUR, EXP-CI-TRAC
PDI-3 *	GDB-CARTO, GDB-QUALIF-SENS
PDI-6 **	EXP-PROT-INF
PHY-2-2 ***	PHY-PUBL, PHY-SENS, PHY-CTRL, PHY-CI-LOC, PHY-CI-MOYENS, PHY-CI-TRACE

Merci de votre attention !

https://www.occitanie-ouest.cnrs.fr/fr

www.cnrs.fr