

- [FR](#)
- [EN](#)
- [ES](#)



Numérique
& innovation pédagogique



Navigation principale

- [Organisation](#)
 - [Stratégie du Numérique](#)
 - [Direction du Numérique](#)
 - [Numérique responsable](#)
 - [Sécurité des Systèmes d'Information](#)
 - [Protection des données](#)
 - [Service Universitaire de Pédagogie](#)
 - [Partenariats](#)
- [Services](#)
- [Projets](#)
- [Ressources](#)
- [Assistance](#)

Rechercher

- [Accueil](#)
- Organisation
- Sécurité des Systèmes d'Information

Sécurité des Systèmes d'Information

Un problème à signaler ? Une question à poser ?

En cas de doute, question, événement, site ou mail suspect...

Adressez-vous directement aux RSSI : rssi@uphf.fr

Description

La sécurité informatique ou plus largement la Sécurité des Systèmes d’Information (**SSI**) fait partie de la stratégie du numérique à l’**UPHF** et de l'**INSA HdF**.

Celle-ci s'applique sur l'ensemble des systèmes d'information de l'établissement (Formation, Pédagogie, Ressources Humaines, Recherche, Financier et Comptable, ...) intégrant les moyens techniques, humains et juridiques.

Elle vise à protéger la circulation, le stockage et le traitement des données afin de garantir la continuité de l’activité de l’université dans un contexte stratégique des données numériques stockées (données scientifiques, données technologiques, données de gestion, données personnelles...).

Les 4 piliers de la SSI



Les 4 piliers de la SSI

Chaîne fonctionnelle SSI

L’organisation de la **SSI** dans chaque ministère est conforme à la directive interministérielle n°901 sur la protection des systèmes d’information traitant des informations sensibles non classifiées de défense.

Au sein de chaque ministère, on trouve

- Un Haut Fonctionnaire de Défense et de Sécurité placé sous l’autorité du ministre (HFDS) :**

Il conseille le ministre en matière de défense et de sécurité. Il anime et coordonne la politique en matière de défense, de vigilance, de prévention de crise et de situation d’urgence et contrôle la préparation des mesures d’application. Il veille à la protection du patrimoine scientifique et technique, anime la politique de sécurité des systèmes d’information et contrôle son application.

- Un Fonctionnaire de la Sécurité des Systèmes d’Information (FSSI) désigné et placé sous l’autorité du HFDS :**

Il anime le pilotage de la **SSI** au sein du ministère, il est le lien avec les **AQSSI** et **RSSI**. Il assure la liaison avec les commissions interministérielles et ministérielles spécialisées en matière de **SSI**.

Au sein de chaque établissement, on trouve

- une Autorité Qualifiée pour la SSI (AQSSI):**

Le chef d’établissement. Il définit la politique de sécurité des systèmes d’information adaptée à son établissement et en fixe les objectifs. Il veille à la mise en œuvre des dispositions réglementaires.

- **Un Fonctionnaire de Sécurité de Défense (FSD adjoint) :**

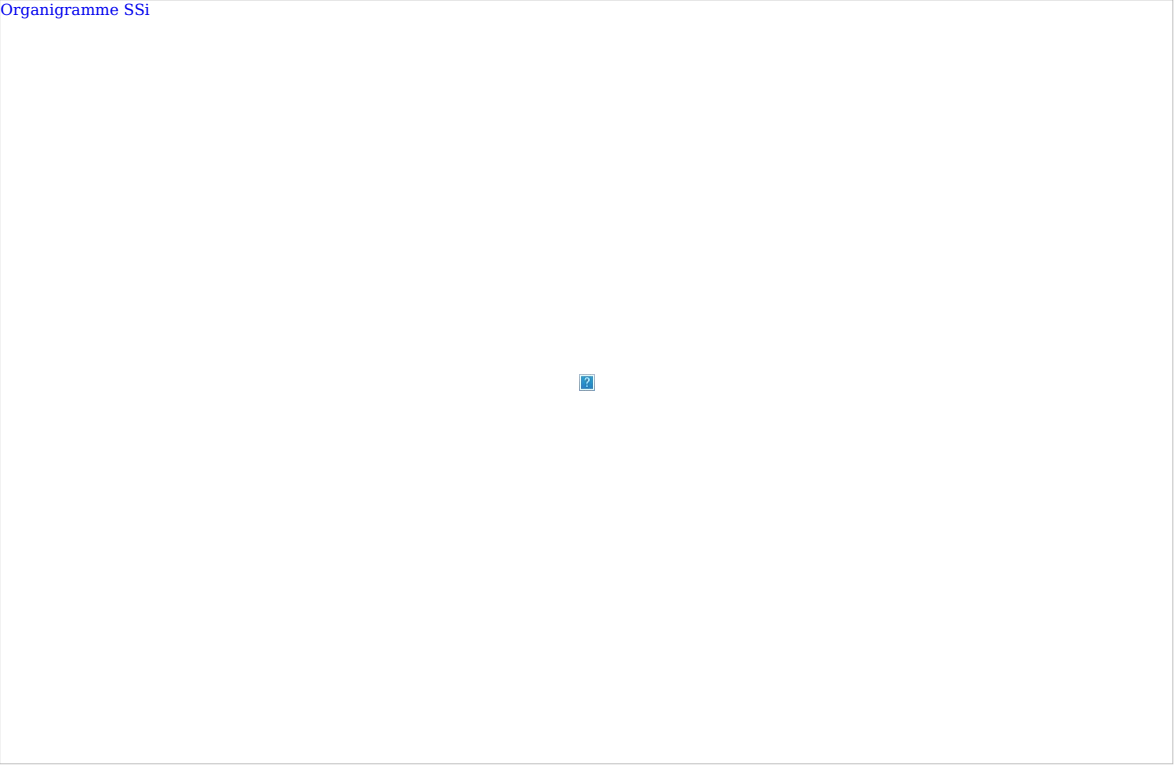
Désigné par l’**AQSSI**, il est le correspondant fonctionnel du **HFDS**, il a un rôle de coordination, de conseil et d’information concernant : la protection du potentiel scientifique et technique, la protection du secret et la préparation/exécution des plans de défense et de sécurité.

- **Un Responsable de la Sécurité du Système d’Information (RSSI) + RSSI adjoint :**

Désigné par l’**AQSSI**, il conseille l’**AQSSI**, assure le suivi des moyens nécessaires à la mise en œuvre des consignes et directives.

[Compléments d'information à retrouver sur le site dédié à la SSI de Renater](#)

Organigramme SSi



[Organigramme de la SSI](#)

Actions mises en œuvre pour la SSI

Sensibilisation

La sécurité informatique n'est pas que l’apanage des informaticiens de la **DNum**, des composantes ou de procédés technologiques, mais bel et bien l'affaire de tous.

C'est pourquoi la **DNum** met en œuvre un plan de prévention à ces risques par une information régulière sur les points saillants des alertes de sécurité et la mise en place d’événements (conférence...) autour de la sécurité numérique.



Affiche de communication sur la cybersécurité

Juridique- Règlement intérieur

Chaque usager de l'établissement : étudiant, personnel administratif, technique, enseignant, chercheur et invité est responsable des moyens numériques (réseaux, machines, plateformes...) mis à sa disposition.

Ces responsabilités, droits et devoirs sont définis dans un acte juridique validé en conseil d'administration de l'**UPHF** et appelé [Règlement intérieur des usages des systèmes d'Information](#).

Il existe également la réglementation **PSSIE** (Politique de Sécurité des Systèmes d'Information de l'État) qui définit les orientations nationales en matière de sécurité des systèmes d'information et à laquelle les ministères et les établissements publics d'État doivent se soumettre.
[Plus d'informations sur la PSSIE](#)

Environnement technologique

L'université met en place un certain nombre de briques technologiques permettant les accès aux systèmes d'information de l'établissement de manière à suivre les recommandations nationales (ex: taille et complexité des mots de passe, accès via VPN, authentification multifacteurs...) et œuvre à consolider les environnements et plateformes dans ce sens.
Vous trouverez ci-contre les trois outils mis en place à l'**UPHF** :

- **ESUP OTP** (authentificateur multifacteur)
- **eduVPN** (VPN)
- **Sésame** (gestion de l'identité numérique, mot de passe, identifiant...]

Logo ESUP OTP



Logo eduVPN



Logo Sésame



Liens recommandés

[Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques](#)
[cyber.gouv.fr](#)

Téléchargements recommandés

[VeraCrypt \(Chiffrement de dossiers de sauvegarde sur supports externes\)](#)



Hauts-de-France
Campus Mont Houy
59313 Valenciennes cedex 9
Tél. : 03 27 51 12 34

[Plan des Campus](#)

- [Services publics +](#)
- [Recrutements](#)
- [Mentions légales](#)
- [Plan du site](#)
- [Crédits](#)
- [Accessibilité : partiellement conforme](#)

[Requête d'amélioration](#)

Saisissez au moins 3 caractères pour voir des résultats