**Séminaire des 10 et 11/04/2018, IFSTTAR Versailles Satory**

# ATELIER

# Sûreté - Défense

# Contexte

La création de l’U-Cible est une très forte opportunité de produire de nouvelles idées et de développer ainsi de nouvelles collaborations.

La sûreté et la défense occupent une place fondamentale dans la gouvernance d’un établissement. Aujourd’hui, chaque entité qui constituera l’université cible a un mode d’organisation et un fonctionnement qui lui est propre en matière de sûreté - défense.

L’atelier sera ainsi un lieu d'échange invitant les participants à se découvrir, à communiquer sur l’existant et à réfléchir sur une organisation harmonieuse en matière de protection de nos biens, de nos personnels (hors sécurité et hygiène du travail) et de nos savoirs et idées.

# Objectif

L’objectif de cet atelier est dans ce contexte de recueillir l’existant (modes d’organisation et pratiques des différents établissements dans les domaines concernés par la sûreté - défense) et de démarrer une réflexion en tenant compte des différents points de vue le plus largement possible :

* Comment est organisée la politique en matière de sûreté – défense, de vigilance, de prévention de crise et de situation d’urgence, de sécurité des systèmes d’information (SSI) dans chaque établissement ?

Existe-t-il des échanges réguliers avec le Haut Fonctionnaire de Défense et de Sécurité (HFDS) et ses services, avec le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), avec l’agence nationale de la sécurité des systèmes d’information (ANSSI), … ? Quels acteurs au sein de chaque établissement : Fonctionnaire de Sécurité et de Défense (FSD), officier de sécurité, Responsable de la Sécurité des Systèmes d’Information (RSSI), ..., et quel temps imparti ?

* Comment est mise en place la protection du Potentiel Scientifique et Technique (PPST) et notamment quelle politique existe en ce qui concerne le recrutement des personnels temporaires ? Des dispositifs sont-ils mis en place pour les zones stratégiques ou sensibles (Zones à Régime Restrictif (ZRR)) ?
* L'application des dispositions relatives à la protection du secret de la défense nationale : comment sont gérées les habilitations au secret, les documents classifiés ?
* La sécurité des échanges internationaux : quelles procédures existent en ce qui concerne les déplacements des personnels à l’étranger (consignes, conseils, ordinateurs dédiées…), la gestion des stagiaires et visiteurs (badges, registres des visiteurs, accès limités aux SI, …), l’accueil de délégations étrangères dans les laboratoires (contrôle des identités, parcours de notoriété, …) ?
* Comment se décline la mise en œuvre ou la conception de dispositions de défense (politique de sûreté des bâtiments, règlement intérieur, plans de défense Vigipirate, plans de continuité d’activité, etc…) ? Comment sont examinées les vulnérabilités de chaque établissement ?
* Sensibilisation des personnels : au sein des différents établissements, les personnels sont-ils sensibilisés aux aspects sécurité défense et intelligence économique ?
* Sécurité des Systèmes d’Information : comment sont mises en place les mesures édictées dans la Politique de Sécurité des Système d’Information de l’Etat (PSSIE) ? (Chartes informatiques, accords de confidentialité, hiérarchisation de l’information, protection contre l’ingénierie sociale, …)

***Rédactrice : Lidwine CRAMPON (IFSTTAR)***