AFCN

AGENCE FÉDÉRALE DE
CONTRÔLE NUCLÉAIRE

AFTERCARE

Personnel interne et externe

Avril 2024

FANC AFCN

FEDERAAL AGENTSCHAP VOOR NUCLEAIRE CONTROLE

AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

Aftercare du personnel interne et externe

Contents

1. Introduction 3
2. Qu'est-ce 'insider threat', pourquoi une menace ? 4
3. Programme Trustworthiness 5
   A. Général 5
   B. Principes de base 6
4. Culture de sécurité 6
   A. Général 6
   B. Interface avec 'IAEA Nuclear Security Series No. 7 Nuclear Security Culture: implementing guide' 7
   C. Rôle de la direction dans la culture de sécurité 9
   D. Mesures concrètes qui peuvent être prises 9
5. «Trustworthiness» suivi du personnel 10
   A. Général 10
   B. Respect de la vie privée 11
   C. Documentation 11
   D. Mesures concrètes à prendre 12
      Actions de pré-emploi : 12
      Employment: 13
      Mesures en cas de doute ou absence de longue durée : 15
      Post-employment/upon termination: 15
6. Human Reliability Programme 15
   A. Politique du personnel 15
   B. Collecte d'informations pour suivre les changements de comportement 15
      Evaluations périodiques 15
      Contact avec la personne concernée 16
      Enregistrement régulier 16
      Rapports 16
      RH communique les modifications à l'OS 16
      Vérification des informations 17
      Contact avec les OS 17

C. Plateforme interne 17
D. Apporter un soutien 18
E. Examen complémentaire auprès de l'ANS 18
F. Une communication claire 18
7. Mécanismes de notification 18
A. Quels types de notifications? 18
Mode de notification 18
Informations à l'informateur 19
B. Mise en commun des informations 20
Plateforme interne 20
Synthèse du message ou des signaux 20
Demande d'informations de base 21
C. Enquête interne 21
D. Mesures 22
Au début ou au cours de l'enquête 22
Après enquête 22
E. Rapports internes (équipe/interne) 22
8. Amélioration continue 23
9. Conclusion 23
ANNEXE A : Signaux qui pourraient indiquer un comportement changeant 25
ANNEXE B : Lien à la recherche doctorale donnant un aperçu des mesures 31
ANNEXE C: Tips & Tricks pour un entretien 32
ANNEXE D: Circulaire CP3 34
ANNEXE E : Exemples de formations 35

1. Introduction

Le présent document est la conclusion du projet « Aftercare pour le personnel interne et externe », dans le cadre de « insider threat ». Les opérateurs nucléaires et les entreprises de transport nucléaire qui travaillent dans les secteurs nucléaire et radiologique doivent tenir compte de « l'insider threat » et élaborer un programme de lutte contre cette menace.

L'objectif de ce projet était d'élaborer des lignes directrices pour l'élaboration de mesures préventives contre un « insider adversary ».

Dans le secteur nucléaire, il existe actuellement une réglementation claire en matière de screening (habilitations de sécurité/attestations de sécurité/autorisations d'accès). Une personne ayant accès aux zones ou informations sensibles des installations nucléaires ou des entreprises de transport nucléaire aura été soumise à un processus de filtrage. Toutefois, le filtrage n'est qu'un instantané, une photographie de la situation d'une personne à un moment donné dans le temps, dans le but d'évaluer le comportement futur d'une personne. Il est donc important de prévoir, en plus du filtrage, des mesures de suivi de la fiabilité d'une personne. La personne peut donc faire l'objet d'un suivi dans le cadre d'un programme de « trustworthiness ».

L'accent sera mis sur le cycle de vie du travailleur. L'objectif est de donner une vue d'ensemble des actions possibles que les installations nucléaires ou les entreprises de transport nucléaire peuvent entreprendre, ainsi que d'indiquer où se situe la frontière avec ce qui peut être fait légalement en ce moment et ce qui n'est pas possible dans le cadre de la vérification/du suivi de la fiabilité d'une personne. Il appartient aux installations nucléaires ou aux entreprises de transport nucléaire de mettre en œuvre au sein de leur installation les mesures qu'elles jugent utiles et de décider à qui ces mesures s'appliqueront. La responsabilité de la mise en œuvre des mesures incombe au secteur. L'AFCN attire également l'attention sur la nécessité de la consultation préalable des partenaires sociaux et d'éventuelles adaptations au règlement de travail.

La première réunion de mars 2021 s'est concentrée sur l'objectif de ce projet, ainsi que sur certains principes fondamentaux à respecter.

La deuxième réunion, qui s'est tenue en février 2022, a permis d'approfondir les principes fondamentaux d'une bonne culture de sécurité nucléaire.

La troisième réunion, qui s'est tenue en décembre 2022, a donné un aperçu des mesures concrètes qui pourraient être prises au cours du cycle de vie des employés.

Lors de la quatrième réunion de juin 2023, nous nous sommes penchés sur les mesures qui pourraient être prises pour assurer le suivi du personnel tout en travaillant dans l'organisation, ainsi que sur les différents partenaires susceptibles de détenir des informations.

Dans la cinquième partie, en novembre 2023, il a été examiné comment ces informations peuvent être suivies et traitées davantage.

Et lors de la dernière réunion du mois de mars 2024 le tout a été consolidé dans un seul document et l'accent a été mis sur l'amélioration continue.

Il s'agit d'une ligne directrice d'accompagnement. Toutefois, il appartient toujours à l'organisation de décider quelles mesures sont mises en œuvre et de quelle manière.

2. Qu'est-ce 'insider threat', pourquoi une menace ?

La menace de son personnel interne (insider) qui, intentionnellement, commet (ou tente de commettre) une action non autorisée, en visant ou en utilisant des matières nucléaires ou autres matières radioactives, ou des institutions, entreprises de transport ou activités associées, est très présente.

Pour la définition de la « menace interne », nous mentionnons la collection 'Sécurité nucléaire' de l'AIEA N°8-G (Rev1). Un 'insider' est considéré comme : "*Une personne ayant un accès autorisé à des matières nucléaires, des installations ou activités nucléaires ou à des informations ou sources d'informations sensibles, qui mène intentionnellement ou facilite une action criminelle ou non autorisée contre des matières nucléaires, d'autres matières radioactives ou des activités associées*".

Plus précisément, un 'insider' a l' « **accès** », l' « **autorité** » et la « **connaissance** » et cette personne peut constituer une menace dès qu'elle a l'intention de commettre ou de faciliter une action non autorisée.

Pour pouvoir se protéger contre une « menace interne », une combinaison de mesures préventives et de protection doit être prise au sein d'une organisation :

- Mesures préventives (avant une action) : pour minimiser le nombre de « menaces internes » possibles et pour réduire la possibilité d'une action non autorisée par un insider ;
- Mesures de protection (après une action) : mesures pour résoudre la situation après une action d'un 'insider' et pour atténuer la gravité de l'action.

Idéalement, les mesures préventives devraient être suffisantes pour empêcher toutes les tentatives d'actions potentielles d'un 'insider', mais malheureusement, il n'y a aucun moyen d'obtenir une vue d'ensemble complète des indicateurs comportementaux qui prédisent l'action d'un 'insider'. Nous observons ici encore un comportement humain, qui reste difficile à prédire. Cependant, des études ont démontré que les actions d'un insider contiennent également des indicateurs visibles au préalable. Ce sont les indicateurs sur lesquels il faut travailler pour mettre en place des mesures préventives. Même s'il est également nécessaire de prendre des mesures de protection, pour les cas où la prévention n'a pas été possible ou non efficace.

La menace interne a également été incluse dans l'analyse 'Design Basis Threat'. La menace concrète y est aussi décrite plus en détail. Cependant, la motivation d'un initié peut varier considérablement, quelques exemples : argent, idéologie, vengeance, ego, menace ou une combinaison de ces facteurs. C'est aussi fortement individuel. La difficulté est de constater qu'une personne commence à développer ou a développé une certaine motivation, afin d'identifier efficacement la menace et de pouvoir agir contre elle.

3. Programme Trustworthiness

A. Général

Un programme de fiabilité examine les comportements ou caractéristiques indésirables ou suspects pour déterminer si quelqu'un peut être une menace. Dans un tel programme, il doit être possible de fournir des garanties que les personnes concernées sont dignes de confiance dans la mesure où ils ne présentent pas un risque déraisonnable pour la santé, la sûreté et la sécurité de l'organisation et des autres membres du personnel.

Cela est très difficile car l'intention d'un insider peut être non visible et les schémas comportementaux d'une personne représentant une menace peuvent différer considérablement ou avoir une autre cause. Cependant, une recherche a montré qu'un certain nombre de comportements ou de caractéristiques peuvent être un indicateur d'une plus grande probabilité qu'un individu entreprenne une action intentionnelle non autorisée. Il s'agit de facteurs internes, externes et contextuels qui poussent la personne vers des actions intentionnelles non autorisées afin de provoquer une réaction.

Certains de ces comportements, liste non exhaustive, sont :

- Problèmes de gestion de la colère
- Association ou sympathie avec des groupes criminels ou terroristes
- Difficulté à accepter les commentaires ou les critiques
- Comportement conflictuel
- Insatisfaction au travail
- Non acceptation de l'autorité
- Abus de drogues ou d'alcool
- Isolement social
- Problèmes financiers
- Réticence à suivre les règles et les procédures
- -...

Un programme de fiabilité comporte plusieurs composants. Il s'agit d'un processus permettant de collecter des informations sur une personne spécifique, d'analyser les informations par rapport à des critères spécifiés et de déterminer si la fiabilité d'une personne peut être suffisamment assurée. Cependant, le comportement et la fiabilité d'une personne peuvent également changer avec le temps. Par conséquent, il est impératif de procéder également à des évaluations adéquates de la fiabilité tout au long de la carrière de la personne.

Cela concerne le suivi des personnes en plus des contrôles légaux prévus par la législation. Le comportement peut changer avec le temps. L'Officier de sécurité a pour rôle de suivre le comportement des personnes pour lesquelles une enquête a été demandée (art. 13/1, par. 1, b. Loi du 11 décembre 1998 [concernant la classification et les habilitations de sécurité, les certificats de sécurité et les conseils de sécurité]). Cependant, l'Officier de sécurité ne peut pas effectuer une surveillance pour tout le personnel. Des mécanismes doivent être mis en place pour lui permettre d'avoir les informations et un cadre doit être créé au sein de l'organisation pour assurer le suivi de ces informations. Cela devra être défini dans des procédures, ainsi que la fonction des personnes qui assureront le traitement de ces informations (ex. RH). S'il s'agit

d'enquêtes sur des personnes en phase de recrutement ou des personnes qui ne sont pas tenues de se soumettre à un contrôle légal, le service RH a un rôle à jouer.

B. Principes de base

Aperçu :

1. Le management a une fonction d'exemple et les principes doivent également être soutenus par le management.
2. Une culture de sécurité soutenue au sein de l'organisation est la base : le personnel doit considérer la sécurité comme sa responsabilité et ainsi remarquer et transmettre les signaux sur les changements de comportement des gens.
3. Le personnel ne doit pas être considéré comme une menace permanente, mais comme un moyen possible de faire face à une menace.
4. La base d'un « programme de fiabilité humaine » est une bonne gestion du personnel : pour s'assurer que les employés ne se retournent pas contre l'organisation, ils doivent être satisfaits de leur environnement de travail.
5. Les personnes doivent être déployées au bon endroit : non seulement en ce qui concerne les capacités techniques mais aussi les traits de personnalité doivent être pris considération (ex. résistance au stress, ...).
6. Une 'approche gradue' doit être utilisée : ne pas déployer toutes les ressources sur tout le monde, mais en fonction des accès, de l'autorité, de la position hiérarchique et des connaissances. Il faut analyser quelles fonctions peuvent causer le plus de dégâts.
7. Un aperçu clair doit permettre de déterminer, par exemple : quels sont les comportements détectables, définir clairement ces comportements (pour éviter également les soupçons), des critères permettant d'assurer la fiabilité d'une personne, mais aussi les réactions possibles à prendre et qui prend quelle décision (enquête complémentaire de l'ANS, éventuelle plainte à la police, changement temporaire de fonction, licenciement, ...) et comment agir rapidement (dans certains cas, une action directe est nécessaire).
8. Règles de confidentialité : les règles de confidentialité applicables en Belgique doivent être prises en compte. Le programme de fiabilité doit être en équilibre avec les droits de la personne. Une bonne description du programme et des mesures possibles sont un bon début.

4. Culture de sécurité

A. Général

Une « culture de sécurité » intégrale est un élément important dans le contexte de 'Aftercare'. Cela devrait être intégré dans la culture d'entreprise globale, afin que cela devienne une habitude pour chacun comme cela est actuellement le cas avec la culture de sûreté.

Si nous examinons les définitions d'une « culture », nous pouvons conclure qu'il s'agit des idées, des habitudes et des valeurs d'un groupe spécifique. Cela signifie que les règles et les principes de sécurité doivent être largement connus et utilisés afin que cela devienne une seconde nature pour les personnes de réagir. L'objectif général est que le personnel interne et externe considère volontairement et consciemment la sécurité comme de leur responsabilité.

Les valeurs du personnel et sa loyauté envers l'organisation (exploitant nucléaire ou entreprise de transport nucléaire) sont des aspects importants dans le contexte de la menace interne ou de « insider threat ». On peut supposer que les personnes qui sont loyales envers leur organisation et qui ont de bonnes mœurs au sein de cette organisation représentent moins une menace, car elles sont moins susceptibles de prendre des mesures pour nuire à cette organisation. Une culture 'no blame' stimulant le dialogue est donc très importante.

Il est important que tout le monde au sein de l'entreprise soit au courant des mesures et procédures de sécurité et soit conscient de l'existence de la menace interne ainsi que des conséquences possibles. La bonne gestion des différentes procédures et la manière dont il faut réagir aux situations est donc l'une des mesures contre « la menace involontaire » (abus de l'accès de quelqu'un, sans que la personne en soit consciente). La formation et l'entrainement de ces procédures et règles sont également nécessaires.

Les formations autour de la menace interne doivent également pouvoir être présentées avec les nuances nécessaires. Tout le monde devrait être conscient de la menace et des conséquences possibles, mais l'objectif n'est pas de se méfier de tout le monde et de voir tout le monde comme une menace. Au sein de cette menace, cependant, il est important d'être conscient du comportement du personnel et que les ajustements à ce comportement ou le comportement suspect soient perçus afin que cela puisse être suivi. Un changement de comportement n'est pas non plus la preuve standard d'une éventuelle menace interne. La personne peut faire face à d'autres problèmes ou défis, de sorte qu'un rapport d'un tel comportement puisse également conduire à l'aide et au soutien nécessaires de la personne. Cela devrait être considéré dans son ensemble. Grâce au signalement, on peut essayer de fournir à la personne le soutien nécessaire, qu'elle ait effectivement commencé à devenir une menace interne ou pas. Le signalement doit devenir une seconde nature et, le plus possible sans qu'il soit nécessaire d'imposer des sanctions afin de permettre également l'auto-signalement (sans que cela ne soit considéré comme une entorse aux règles).

Il est donc également important que des mesures puissent être prises le plus tôt possible lorsqu'il est observé que quelqu'un pourrait devenir une menace interne. Sans qu'une action ne soit entreprise, tout peut encore être évité et la personne peut encore ajuster son comportement. Il est important que les collègues directs soient en mesure de discuter entre eux de tels ajustements de comportement ou d'inconduite et de pouvoir le signaler. Cela fait partie de la « culture de sécurité ». Il faut également être conscient du suivi des rapports, afin de savoir que l'information sera correctement traitée et consultée. Il s'agit d'empêcher que les gens n'osent rien signaler par crainte de sanctions.

B. Interface avec 'IAEA Nuclear Security Series No. 7 Nuclear Security Culture: implementing guide'

Si nous examinons les directives de l'AIEA sur la « culture de sécurité », nous arrivons au diagramme suivant :

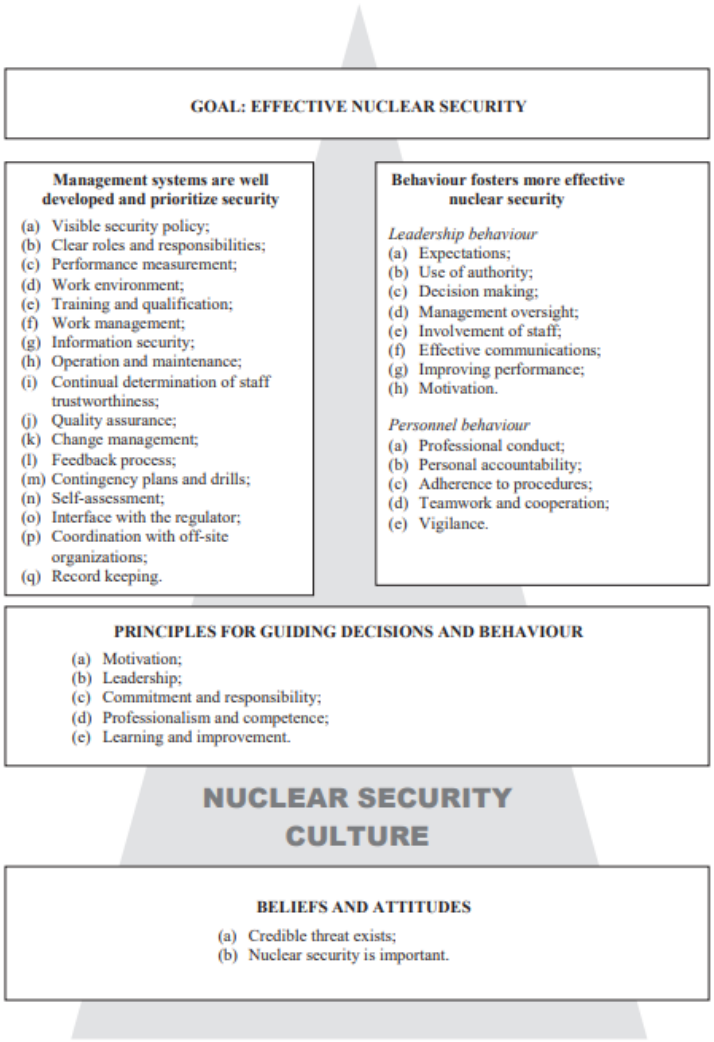

FIG. 2. Characteristics of nuclear security culture.

Il est clair que certains aspects ont un impact direct sur la notion de « Aftercare », nous pensons principalement à :

- Rôles et responsabilités clairs : le rôle de tous les membres de l'organisation doit être expliqué ainsi que le rôle du suivi de l'information communiquée ;
- Environnement de travail : lorsqu'une personne travaille dans un bon environnement et qu'elle se sent loyale envers une organisation, elle est moins susceptible de constituer une menace pour l'organisation ;
- Formation : une sensibilisation et des conseils doivent être fournis sur la menace interne et « aftercare » ;
- Suivi continu concernant la fiabilité : toutes les personnes au sein d'une organisation sont responsables du comportement de chacun. En cas de doute ou de changement de comportement, cela doit être signalé pour une enquête plus approfondie ;
- Comportement de leadership : la direction doit donner l'exemple pour renforcer la culture de sécurité (plus d'informations à ce sujet dans la section C) ;

- Comportement du personnel : l'organisation est soutenue par le personnel. Il est donc important que chacun sache quel comportement est attendu d'eux et qu'ils considèrent la sécurité de l'organisation comme leur responsabilité, pour s'assurer que les procédures soient suivies. Il faut déterminer la frontière entre un comportement considéré comme acceptable et un comportement considéré comme inacceptable ;
- Croyances et comportements : cela reste le fondement de toute la culture de sécurité.

La culture de sécurité doit donc être ancrée dans l'organisation et le rôle et la responsabilité de chacun doivent y être assumés. Il est également important que ce ne soit pas un sujet soutenu uniquement par le département de sécurité, mais également et avant tout démontré par le management de l'organisation. Ceux-ci doivent s'assurer qu'il y ait suffisamment de ressources (humaines et financières) et d'aménagement pour encourager cette culture de sécurité. Des procédures et des structures suffisantes doivent donc être mises en place mais il est aussi nécessaire de veiller à permettre la formation et le suivi des informations communiquées.

La « culture de sécurité » devrait également être évaluée régulièrement afin de permettre une amélioration continue. Ici aussi, il existe des directives de l'AIEA sur « l'auto-évaluation » de la culture de sécurité (NSS n° 28-T), qui peuvent étayer cette évaluation.

C. Rôle de la direction dans la culture de sécurité

La culture de sécurité doit être soutenue par tout le monde. L'information doit remonter du bas vers le haut et doit aussi être signalée dans toute l'organisation dans le cas où certaines mesures ne sont pas efficaces afin que celles-ci puissent être adaptées. Il est aussi important d'inclure une approche « top down », sinon cela ne réussira pas. Ce n'est donc pas seulement la responsabilité du département de la sécurité, mais aussi de la haute direction et de tous les autres départements qui doivent jouer leur rôle à cet égard.

La direction doit également prendre en compte la sécurité et ajuster son comportement en conséquence, afin que tout le monde au sein de l'organisation prenne cela en considération avec l'importance adéquate. Compte tenu de leur position hiérarchique, il est nécessaire qu'ils gardent eux-mêmes une vue d'ensemble de la fiabilité du personnel de l'organisation, tant interne qu'externe.

Un système de gestion avec des responsabilités, des rôles et des procédures clairs pouvant soutenir cela, est nécessaire. Une ligne directrice des comportements et des attentes rendra plus efficace le suivi continu de la fiabilité du personnel. Concrètement, cela peut aussi donner une image plus claire des comportements et des caractéristiques à surveiller (voir annexe A), tels que comportement professionnel, responsabilité personnelle, suivi des procédures, travail d'équipe, coopération, prudence, etc.

D. Mesures concrètes qui peuvent être prises

Vous trouverez ci-dessous un aperçu des mesures qui peuvent être prises dans le contexte de la culture de sécurité pour soutenir ce sujet :

- Formation + sessions de formation : lors de l'entrée dans l'organisation, avec les rappels nécessaires. Cela devrait également être prévu pour le personnel externe :
    - Qu'est-ce que l'insider threat ?
    - Motivation possible

    - Rôle de chacun dans ce domaine – responsabilité de chacun
    - Soutenir les collègues et répondre aux problèmes éventuels des collègues
    - Mesures prises à cet effet : restriction de l'accès, répartition des tâches, règle de deux personnes, ...
    - Impact possible
    - Grâce à l'identification précoce : de l'aide peut être offerte à la personne, aucune conséquence pour la personne et pour l'environnement
- Campagnes de sensibilisation
    - Porter un badge
    - Aspects cyber → Maintenu à jour
    - Rapporter
    - ...
- Externes :
    - Coopération entre les officiers de sécurité
    - Inclure dans les contrats qu'il faut prêter attention à cela
    - Inclure la formation
- Politique générale RH : mettre l'accent sur le moral du personnel et avoir une bonne politique
    - De bonnes personnes au bon endroit, non seulement en regardant les connaissances, mais aussi les traits de personnalité par rapport au poste
    - Bon environnement de travail
- Évaluation de la culture de sécurité : évaluation périodique des différents aspects de la culture de sécurité

5. «Trustworthiness» suivi du personnel

A. Général

Il est préférable que ces mesures soient prises dans le cadre d'une approche graduée. Cela implique une analyse de qui a accès à quoi (matériel, documents et zones) et des connaissances qu'ils possèdent dans le cadre de leurs fonctions (établissement d'un profil de risques). Sur cette base, il est possible de déterminer quelles personnes doivent être suivies plus que d'autres.

Cette analyse peut se faire sur la base des fonctions et des accès spécifiques liés à ces fonctions. Dans un second temps, il est possible d'augmenter ou d'étendre les mesures si une personne a déjà occupé plusieurs postes et dispose donc d'un niveau de connaissances plus élevé nécessitant une attention particulière. L'objectif est de lier les mesures au risque et à l'impact des conséquences d'un acte délibéré.

L'objectif d'un programme « trustworthiness » est de déterminer si une personne est fiable, de suivre le personnel pour détecter les changements de comportement, mais il peut également avoir un effet dissuasif (lorsque l'on sait que l'adaptation du comportement sera observée). Les mesures de « trustworthiness » peuvent préférablement être prises : pour le recrutement, pendant les activités professionnelles et à la fin de celles-ci. Il s'agit d'une combinaison de différentes mesures en fonction de la situation. Le secteur nucléaire fait déjà l'objet d'une procédure d'examen par les pouvoirs publics. Le présent document dresse une liste des

mesures supplémentaires qui pourraient être prises. Il convient de poursuivre l'examen, par organisation, des mesures qui peuvent être soutenues et mises en œuvre (et de quelle manière).

B. Respect de la vie privée

Ces mesures supplémentaires, en plus des screenings légaux existants, ne peuvent être mises en œuvre qu'à des fins spécifiques et explicites, en l'occurrence la protection contre les menaces internes. L'employeur a un intérêt légitime à procéder à certains contrôles. À cet égard, il doit informer suffisamment les travailleurs ou le candidat (dans le cadre du pré-emploi) de tous les aspects des mesures accessoires (objectifs, délais de conservation, actions possibles, etc.). La documentation relative à ces processus (voir section C) est déjà importante lors d'une candidature et doit toujours être communiquée.

Pour chaque mesure, il est important de préciser la finalité et donc d'avoir une vue d'ensemble des données traitées. Dès que l'employé n'est plus employé au sein de l'organisation, le traitement des données doit cesser.

Ces mesures doivent toujours tenir compte du principe de proportionnalité et, comme nous l'avons déjà mentionné à plusieurs reprises, nous suivons les principes d'une approche graduée.

Au cours de ce processus, il convient de veiller à ce que le profilage ne soit mis en place[1] que dans les cas d'exceptions prévus par la loi en matière de protection de la vie privée. Lors de l'analyse, une intervention humaine restera toujours nécessaire.

Il est important de respecter les exigences de la législation en matière de protection de la vie privée dans le cadre de ce processus.

C. Documentation

Il est important de préciser qui est responsable du programme « trustworthiness ». En vertu de la législation qui s'applique au secteur nucléaire, il appartient à l'officier de sécurité de suivre les personnes en possession d'une habilitation de sécurité/d'une attestation de sécurité. Toutefois, l'officier de sécurité doit être soutenu par l'organisation à cette fin, faute de quoi cela ne peut se faire de manière efficace. À cette fin, l'officier de sécurité peut collaborer avec le service de sécurité, les RH, la ligne directe avec le management et toute autre personne au sein de l'organisation ayant des contributions pertinentes.

Il est important que tous les processus, responsables, actions et rapports soient bien documentés. L'ouverture la plus large possible aux différents processus et activités permettra de renforcer la confiance du programme. Dans pareille collaboration, il convient de déterminer à l'avance qui a accès à quelles informations et où elles sont stockées, afin que chacun en soit informé.

Le personnel doit donc être suffisamment formé et obtenir toutes les informations nécessaires pour prendre des mesures supplémentaires si nécessaire.

[1] Tout traitement automatisé de données à caractère personnel consistant à évaluer, à l'aide de données à caractère personnel, certains aspects personnels d'une personne physique, notamment en vue d'analyser ou de prévoir le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements d'une personne physique.

Un programme comme celui-ci devrait être évalué régulièrement afin d'identifier les défis et les difficultés et de faire en sorte que tout soit mis en œuvre de la manière la plus efficace possible.

Les mesures décrites dans le présent document concernent la collecte d'informations. Nous poursuivrons ensuite le projet en ce qui concerne les suggestions de communication d'informations, l'analyse des données et les actions éventuelles.

Il est important de veiller à ce que toutes les mesures complémentaires soient les mêmes pour tous, c'est-à-dire qu'elles sont liées à certaines fonctions (« approche graduée »). Les mesures retenues devraient être suffisamment détaillées dans le règlement du travail, le contrat et la déclaration relative à la protection de la vie privée. Toutefois, il appartient à l'exploitant nucléaire ou à l'entreprise de transport nucléaire de déterminer quelles mesures peuvent être prises dans le cadre de leur programme « trustworthiness » et donc être élaborées au sein de l'organisation.

D. Mesures concrètes à prendre

Actions de pré-emploi :

- Veuillez vérifier le contexte :
    - Vérification de l'identité : éventuellement via du matériel spécifique permettant la vérification de la carte d'identité ;
    - Examen de l'historique du travail du travailleur[2] : demander de compléter un document reprenant les employeurs précédents et leurs coordonnées ainsi que son autorisation pour vérifier les données ;
    - Vérification open source/réseaux sociaux : les données peuvent être consultées, mais soyez prudent lors du traitement ultérieur de ces données ;
    - Demande du casier judiciaire : le document de base peut être consulté et examiné. Il ne peut pas être traité ultérieurement ;
    - Audit financier : un extrait des fichiers CCP (Centrale des Crédits aux Particuliers) et ENR (Enregistrement non régis) peut être demandé. Il s'agit toutefois d'informations supplémentaires, car elles ne peuvent pas être utilisées spécifiquement pour exclure quelqu'un. Les biens d'une personne sont protégés par la législation en matière de discrimination du 10 mai 2007[3].

[2] Position de l'APD : Le candidat donne son accord en signant une déclaration dont il comprend clairement la portée et qui contient au moins les déclarations suivantes :

1. son identité et celle des organismes ou personnes que l'employeur souhaite consulter ;
2. la nature des données demandées ;
3. les raisons de la collecte des données ;
4. la période pendant laquelle le consentement sera utilisé.

Si une personne de référence est mentionnée dans le CV, cela peut être considéré comme un consentement du candidat. En tout état de cause, l'employeur ne pourra pas vérifier systématiquement auprès de tiers les informations que le candidat lui a transmises. Si un CV présente des lacunes évidentes, l'employeur doit d'abord interroger le candidat sur ces « lacunes » évidentes dans son parcours éducatif et professionnel. Ce n'est que si l'explication du candidat sur le sujet n'est pas suffisante que l'employeur potentiel peut envisager de collecter des données auprès d'autres personnes ou organisations, à condition que le candidat ait été informé au préalable et ait donné son consentement.

[3] 10 MAI 2007 - Loi tendant à lutter contre certaines formes de discrimination

=> Remarque du secteur : seule une checklist validant la consultation des informations ci-dessus serait conservée, les documents comportant les données à caractère personnel seraient quant à eux détruits.

- Enquête par un détective privé ; à déterminer à l'avance pour quelles fonctions spécifiques et quelles informations sont pertinentes
- Vérification des compétences et du comportement de la personne, afin de s'assurer qu'ils sont conformes à l'emploi, éventuellement au moyen d'une évaluation personnalisée ou d'un entretien approfondi sur les compétences recherchées ;
- Processus d'examen analytique documenté (y compris en tant que volet « awareness ex ante ») : demander l'autorisation de se soumettre à un « Trustworthiness check » et indiquer que des enquêtes seront menées et qu'il y aura un suivi continu du comportement de la personne (il est conseillé de l'inclure dans le contrat de travail) ;
- Examen positif (attestation de sécurité/autorisation d'accès/habilitation de sécurité) requis pour le contrat ;
- Formation de ceux qui recrutent dans le domaine de l'insider threat et de la reconnaissance des signaux relatifs à des comportements suspects ;
- Documentation du processus de recrutement afin d'accroître la transparence ;
- Documentation des décisions prises dans le cadre d'un processus de recrutement ;
- Jury de recrutement composé de différents acteurs de l'organisation ; et
- Liste claire et cohérente des condamnations et des comportements (si possible) qui ne sont pas acceptés en fonction des responsabilités.

=> Exemple du secteur : mettre en place un service distinct (ou faire appel à un détective privé) qui consulte/demande certaines informations afin d'établir un avis de 'sécurité'. Cela permet une certaine indépendance des services RH et ces conseils peuvent être utilisés pour continuer à travailler dans le cadre du processus de recrutement. Le casier judiciaire, par exemple, peut alors être traité séparément.

Employment:

- Transparence :
    - Possession d'un « code de conduite » clair : rendre accessible un bref aperçu, pas seulement un ensemble de règles
    - Vue d'ensemble de toutes les mesures prises dans le cadre du projet d'insider threat : accroître la transparence
    - Système de communication d'informations bien connu : à propos de vous-même et d'autres personnes.
    - Des procédures claires concernant les mesures prises et les enquêtes ouvertes au moment de l'obtention d'informations = enquête administrative + droits que la personne peut faire valoir elle-même.
- Différents mécanismes de communication d'informations ;
- Créer une culture de soutien plus ouverte ("no blame culture") ;
- Système de tutorat/coaching/médiateur permanent pour assurer un suivi direct et continu dans le cadre de la formation, mais aussi dans le cadre du suivi ;

- Briefings de sécurité annuels obligatoires : basé sur les habilitations de sécurité et comment traiter les informations, conséquences possibles en cas d'abus, aspects liés à la culture de sécurité, Menaces Internes (Insider Threats)
- Formation des salariés et de la direction à l'identification des « red flags », culture de la signalisation résultant de la formation à la détection et à la signalisation des signaux d'alarme dans leur contexte et définition des moyens de signalisation, y compris par l'utilisation des → POC (Person of Contact) : informer les travailleurs qu'ils peuvent soutenir leurs collègues et faire part de leurs préoccupations.
- Création d'une équipe 'insider threat mitigation' : gestion, sécurité (responsable de la sécurité), IT, RH, service juridique ;
- Système concret de suivi pour la transmission systématique des modifications en interne et à l'ANS : changement d'adresse, changement de situation familiale, voyages à l'étranger ;
- Des réunions permanentes récurrentes avec chaque membre du personnel, accompagnées d'une analyse de son fonctionnement fiduciaire, sur la base des éléments suivants :
    - Checklist
    - Questionnaire standard basé sur des critères objectifs
- Suivi du comportement numérique des personnes (accès aux zones, documents, comportement de navigation, ...) ;
- Demande systématique du casier judiciaire tous les X ans : le document de base peut être consulté et examiné ; il ne peut pas être traité ultérieurement (à prévoir dans le règlement de travail + justification nécessaire) ;
- Possibilité de réunions à partir d'informations obtenues : information déclarée (par la personne elle-même ou par l'intermédiaire d'une autre personne) ;
- Rencontre récurrente avec une équipe identifiée pour discuter, le cas échéant, de personnes/incidents : sur la base de statistiques générales et de la question de savoir si certaines personnes ont fait l'objet de signalements récurrents. Y compris les informations générales détenues par les RH (accorder une attention particulière à un conflit d'intérêts) ;
- Procédure de recours en cas de désaccord avec la direction ;
- Clarté quant à la possibilité de rencontrer des personnes de confiance ;
- Clarté sur les possibilités d'analyse psychosociale ;
- Systèmes de signalement des personnes de confiance et d'analyses supplémentaires ;
- Limitation de l'accès des travailleurs pour des raisons spécifiques qui doit être clairement définie ;
- Audit des systèmes et accès ;
- Principes des 4 yeux ;
- Systèmes d'alarme sur les systèmes d'accès ;
- Accès sécurisé aux systèmes numériques connectés ;
- Répartition spécifique des rôles et responsabilités ;
- Dans des cas spécifiques on peut, dans des situations documentées, travailler avec un détective privé.

-

Mesures en cas de doute ou absence de longue durée :

- Restriction de l'accès (sur une base générale, qui doit être documentée) ;
- Transmission des informations complémentaires à l'ANS et demander une enquête supplémentaire ;
- Mesures supplémentaires (réunion trustworthiness supplémentaire, ...).

Post-employment/upon termination:

- Un plan clair d'«off-boarding»
- Documentation d'une procédure de licenciement
- Refus d'accès, tant physique que numérique (à cet égard, il convient également d'établir une distinction dans la procédure entre la résiliation forcée et la résiliation volontaire du contrat de travail) ;
- Restitution de tous les équipements de travail de l'organisation (badges, équipement informatique, ...)
- Clause/contrat de confidentialité

6. Human Reliability Programme

A. Politique du personnel

Le travailleur doit être soutenu dans son travail. Il s'agit notamment de mettre en place une politique du personnel qui permette aux personnes d'être entendues et écoutées en créant des relations humaines solides, orientées personnel.

À cette fin, il convient de mettre en place les moyens nécessaires pour faire face aux aspirations du personnel et de mener ensuite des actions dans la mesure du possible. Toute personne au sein de l'organisation doit être en mesure de transmettre des observations sur la manière de travailler, sur les collaborateurs et sur la ligne hiérarchique. Il s'agit également de prendre en compte les modalités prévues par la législation relative à la politique du personnel.

Les modalités d'être entendues doivent être suffisamment expliquées. Il s'agit de veiller à ce que celles-ci soient accessibles et que la communication des informations soit facile, afin de permettre la diffusion de ces modalités. Cela s'appuiera également sur les possibilités d'établissement de rapports.

Les membres du personnel doivent se sentir bien au sein de leur organisation afin de réduire la probabilité d'actions visant à nuire à l'organisation. Cela commence par une bonne politique des ressources humaines et une culture de soutien. Dans le cadre des mesures visant à lutter contre 'l'insider threat', cela aide de déployer les employés à la bonne place, non seulement avec les connaissances requises, mais aussi dans un environnement qui leur convient.

B. Collecte d'informations pour suivre les changements de comportement

Evaluations périodiques

L'évaluation périodique de tous les travailleurs est une méthode permettant le suivi régulier du bien-être d'une personne, de son ressenti au travail et de l'exécution de ses tâches. Cela donne à un N + 1 la possibilité d'avoir des contacts réguliers et, de préférence, bons avec les collaborateurs et de préciser, le cas échéant, certaines actions ou comportements. Cela permet

également de mesurer éventuellement des changements de comportements qui peuvent alors être mis en rapport avec certaines circonstances spécifiques pouvant expliquer ces modifications ou pas. Ceux-ci étant notifiés via des rapports, c'est une mesure visant également à lutter contre la subjectivité et l'arbitraire.

Ces évaluations doivent être documentées et le processus fréquemment rappelé afin que le membre du personnel en soit informé. Cela permettra à la personne d'évaluer ses propres actions sur le lieu de travail et, le cas échéant, d'indiquer si quelque chose peut être modifié.

Des entretiens réguliers permettent de mieux détecter les changements de comportement ou de réaction. Effectivement, ces changements pourraient être moins perceptibles dans le cours normal des choses, étant donné que l'accent est souvent mis sur le résultat du travail.

Des évaluations périodiques peuvent également être effectuées sur les données communiquées par la personne elle-même. Par exemple, un contrôle des médias sociaux est effectué lors du recrutement.

Contact avec la personne concernée

Outre des consultations et des évaluations périodiques, il devrait toujours être possible de consulter une personne en cas de doute quant à certaines actions ou à certains comportements. L'organisation doit veiller à ce que la culture d'entreprise le permette et l'inclure dans ses processus.

Enregistrement régulier

Outre les informations fournies par la personne elle-même, il est toujours utile de disposer de systèmes de surveillance pour signaler les anomalies. Il s'agit principalement de journaux d'accès ou de tentatives d'accès. Il va de soi que les systèmes qui signalent eux-mêmes les anomalies facilitent le processus.

Rapports

Le suivi des données reçues par l'intermédiaire du mécanisme de notification est garanti.

RH communique les modifications à l'OS

L'officier de sécurité (OS) est tenu de transmettre à l'Autorité nationale de sécurité (ANS) les modifications de la situation de vie d'une personne, si elle est en possession d'une habilitation de sécurité. Par défaut, ces modifications doivent déjà être transmises à RH pour le dossier personnel (tenant compte du délai de conservation maximal). La mise en place d'un système systématisé par lequel ces données sont transmises à l'officier de sécurité par l'intermédiaire des ressources humaines peut faciliter ce processus. Cela peut garantir que ces modifications sont systématiquement communiquées à l'ANS. Voici quelques exemples :

- Modifications de l'état civil
- Changements d'adresse

La communication entre la RH et le OS permet de s'assurer que les données sont inscrites à l'endroit correct. Il y a lieu de définir de manière suffisamment détaillée les données à transmettre.

Vérification des informations

Il est évidemment important de vérifier toutes les informations recueillies afin de s'assurer qu'il n'y aura pas de fausses accusations dans le cadre de comportements suspects. La vérification dépend des informations elles-mêmes. Un entretien avec la personne ou la vérification de données auprès d'autres sources sont des processus qui peuvent être mis en place.

Contact avec les OS

Compte tenu du nombre de sous-traitants, une communication active avec les OS des entreprises est également une source d'information. Ces OS ont les mêmes obligations de suivi des employés. L'expérience montre que cela ne se passe pas toujours sans heurts. Cependant, une bonne relation avec les différents OS et l'échange d'informations peuvent également rendre discutables les doutes éventuels sur les employés des sous-traitants.

C. Plateforme interne

Il peut être utile à l'organisation de créer une plateforme interne permettant de réunir des partenaires afin de discuter plus avant d'éventuels « red flags ». Cette plateforme doit permettre de prendre des mesures en fonction du résultat des discussions. Cette plateforme peut se réunir périodiquement pour mettre en évidence les risques éventuels ou se réunir de façon ponctuelle pour des dossiers urgents.

Les partenaires réunis sont les ressources humaines, la sécurité et le bien-être au travail. En fonction du dossier, les N + 1 ainsi que le DPP ou d'autres personnes spécifiques peuvent être entendus.

Cet organisme doit alors être suffisamment connu et documenté. Le cadre dans lequel ils travaillent doit tenir compte de la législation applicable en matière de protection de la vie privée. Il est également important de mesurer les intérêts potentiels (principe de prudence en sécurité).

Sur cette plateforme, des actions et des « red flags » de personnes spécifiques peuvent être discutés. Cela permet de regrouper des données provenant de différents services. A titre d'exemples :

- Rapports de notification
- Enregistrement de l'accès (physique, digital)
- Données des évaluations périodiques
- Données connues auprès des RH
- ...

Veuillez noter que les données qui sont partagées ici doivent être pertinentes pour déterminer si une personne représente ou non une menace interne potentielle. Il convient de définir clairement les critères sur la base desquels un dossier sera présenté. La liste des « red flags » peut, le cas échéant, être prise en considération.

Il est important de rendre compte sans ambiguïté de cette analyse et des conclusions. Il s'agit d'indiquer que l'analyse a été effectuée correctement et de façon objective. Cela peut être ajouté au dossier personnel de la personne elle-même.

D. Apporter un soutien

Les problèmes ou défis d'un employé en dehors du cadre professionnel ne relèvent bien sûr pas de la responsabilité de l'employeur. Toutefois, si cela peut avoir une incidence sur son travail ou sur la fiabilité de cette personne, il s'agit là d'un élément à prendre en considération et auquel l'employeur doit être attentif.

Il est intéressant, le cas échéant, d'avoir une vue d'ensemble des organisations qui apportent une aide sur ce sujet dans la région. Il s'agit, dans un premier temps, d'informations destinées à soutenir l'employé.

Ces organisations peuvent, dans certains cas, contribuer à l'interprétation des signaux suspects. Cela peut également permettre de favoriser la coopération ou le contact avec la personne concernée.

E. Examen complémentaire auprès de l'ANS

En cas de doute sérieux, il est possible de demander un examen complémentaire. Pour ce faire, l'officier de sécurité doit prendre contact avec l'ANS. La possibilité est laissée à l'appréciation de l'OS. Puis, c'est l'ANS qui prend le relais à savoir si les informations sont suffisantes.

F. Une communication claire

L'aspect le plus important, dans ce processus et dans le suivi de la fiabilité d'une personne, est la communication qui s'articule autour de ce processus.

D'une part, les processus et procédures dans ce cadre doivent être bien documentés. D'autre part, cela doit être communiqué à tous les membres de l'organisation.

Si des dossiers spécifiques sont en cours, il doit y avoir une communication suffisante à ce sujet avec la personne concernée ou la personne qui a fait la déclaration. Dans cette communication, la fiabilité des données et la vie privée des personnes concernées sont prises en compte. Si nécessaire, et selon le dossier, la seule notification qu'il en a été fait quelque chose suffit. Cependant, cela doit toujours être pris en considération pour permettre les rapports futurs.

7. Mécanismes de notification

A. Quels types de notifications?

Il est particulièrement important d'essayer de détecter les signaux de changement de comportement le plus tôt possible. Il s'agit de signaux émis par des travailleurs ayant accès au site nucléaire ou à l'entreprise de transport (salariés permanents et employés par un sous-traitant permanent ou non). Toute personne au sein de l'organisation doit en être informée et participer à la collecte et à la diffusion de ces signaux, précisément pour aider l'organisation et la personne concernée. Il s'agit d'une observation par des pairs de situations qui semblent sortir du contexte habituel. Généralement, le processus qui conduit une personne à devenir une menace interne suit certaines phases observables extérieurement, même s'il s'agit de plusieurs instantanés.

Mode de notification

À cet égard, il peut contribuer à faire en sorte que certains dossiers soient automatiquement signalés : il peut s'agir, par exemple, de tentatives de consultation de documents sans autorisation ou d'accès à certaines zones à des moments inhabituels. Il est toutefois important

que tout le monde au sein de l'organisation soit attentif à ces signaux et ait la possibilité de transmettre l'information facilement lorsqu'il y a le moindre doute. Il est recommandé de mettre en place des systèmes accessibles et des processus clairs sur la manière de gérer ces doutes et ces informations. Ces signaux devraient être suivis et la personne concernée devrait bénéficier d'un soutien plutôt que d'être sanctionnée (voir également la loi 'lanceurs d'alerte'[4]). D'un autre côté, l'organisation doit être ouverte à cette fin.

À cet égard, il est recommandé de prévoir diverses possibilités de notification de ces éléments, y compris la possibilité de transmettre les données de manière anonyme. Des niveaux adéquats de sécurité et de protection des données des systèmes doivent être pris en compte pour garantir l'intégrité des données (en tenant compte également de la législation en matière de classification et de catégorisation, si nécessaire). Voici quelques options possibles :

- Formulaire en ligne ;
- Adresse électronique permanente ;
- Formulaire papier dans une boîte (boîtes à plusieurs endroits, et régulièrement vidées);
- Des moments fixes pour parler de soi-même et du service ;
- Personnes de confiance ;
- Cadres.

Il est utile de déterminer les informations que vous souhaitez obtenir lors d'une telle notification, afin d'être en mesure de les examiner. Par exemple, dans le cas d'un formulaire en ligne, vous pouvez le rendre obligatoire (sans que l'auteur de signalement ne soit tenu de s'identifier). Vous trouverez ci-dessous des exemples de données obligatoires :

- Le nom de la personne concernée qui fait l'objet d'une déclaration ;
- Comportement observé ;
- Le moment où cela a été observé ;
- L'endroit où cela a été observé ;
- La raison pour laquelle la personne ayant observé le fait, a des doutes ;
- …

Ces éléments de base vous permettront de poursuivre les recherches en interne, voire de transmettre ces informations à un niveau supérieur. S'il n'y a pas suffisamment d'éléments pour démarrer, on peut se demander s'il est nécessaire d'aller plus loin. Il faut veiller à ce que des informations inadéquates ne soient pas complétées par des hypothèses.

Informations à l'informateur

Il est important d'examiner quelles informations peuvent être transmises à l'informateur (en tenant compte de la possibilité que l'informateur soit anonyme ou ne souhaite pas avoir de contact à ce sujet). Un message automatique ou un aperçu des prochaines étapes peut contribuer à une communication efficace et pertinente ainsi qu'au maintien de la confiance.

De plus, il est possible d'indiquer que les informations feront l'objet d'un suivi qui n'aura pas d'incidence sur l'informateur. S'il s'avère par la suite qu'il s'agit de fausses accusations, l'auteur de signalement peut bien entendu être contacté pour l'informer et, si cela est souhaitable et

[4] 8 DECEMBRE 2022. - Loi relatif aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée

possible, prendre d'autres mesures dans le cadre du contrat de travail (des signalements injustifiés peuvent être considérés comme une faute grave, une fraude, etc.).

Il est nécessaire de rappeler aux employés des installations et transporteurs nucléaires qu'observer et détecter le plus tôt possible des personnes pouvant potentiellement devenir ou être une menace interne permet de réagir et de concevoir pour eux un suivi individualisé dans une démarche positive.

B. Mise en commun des informations

Plateforme interne

La meilleure façon de recevoir les notifications elles-mêmes est un point central/plateforme. Il s'agit de veiller à ce que tous les signalements puissent être traités de la même manière et à ce que tous les canaux d'informations supplémentaires soient clairs. Cela peut permettre de lancer un dossier par notification entrante, précisément pour traiter toutes les notifications de la même manière et avoir une vue d'ensemble de ce qui est fait.

Il est préférable de commencer par examiner la notion 'd'indépendance'. Si une personne de l'équipe chargée de traiter le signalement est trop étroitement liée à l'informateur ou à la personne concernée, il convient de vérifier si cette personne peut continuer à faire partie de l'enquête interne. Pour ce faire, il est plus facile de définir un petit groupe de différents services constituant la plateforme.

De plus, afin que ce mécanisme reste souple, il est préférable que cette plateforme ne se réunisse qu'à la demande de l'un de ses membres ou lorsqu'un cas individuel doit être examiné. Le reste du temps, la plateforme peut être « dormante ».

Cependant, pour un bon fonctionnement, il est nécessaire de déterminer une personne qui prendra la responsabilité d'assurer, au sein de cette plateforme, la coordination et l'accompagnement des différentes mesures prises par celle-ci ainsi que le suivi de la situation.

Synthèse du message ou des signaux

Avant d'ouvrir une enquête, il convient de vérifier si la notification est recevable. Questions pouvant être posées :

- Anonymat : pouvons-nous vérifier efficacement cette notification ?
- Participation : l'informateur est-il à proximité de la personne concernée pour que le signalement puisse réellement être le sien OU ce signalement donne-t-il un effet positif direct à l'auteur de signalement ?
- L'information : existe-t-il suffisamment d'informations ou est-il possible d'obtenir ou de rechercher de plus amples informations ?

En cas de manque d'informations pour aller plus loin, il peut être décidé de ne pas poursuivre une enquête. Cela sera également en lien avec le résultat de l'évaluation des risques déterminant la poursuite ou non d'une enquête.

L'information reçue doit être objectivée autant que possible. C'est un exercice difficile, car les personnes sont invitées à signaler leurs observations, de sorte à ce que le rapport reçu puisse refléter le sentiment d'une personne, ou une situation ou l'illégalité est ressentie. L'objectif est de rendre la plainte aussi objective que possible et de déterminer de quoi il s'agit. Définir des catégories de plainte peut faciliter cette tâche. Quelques exemples :

- Changement de comportement

- Ne pas suivre les règles
- Différend
- …

Demande d'informations de base

Une fois que la notification sera examinée plus avant, il peut être utile d'obtenir quelques données de base en vue d'une enquête interne plus approfondie, par exemple :

- Données des RH ;
- Les plaintes éventuelles à l'encontre de la personne ;
- L'évaluation de la personne.

L'utilisation d'un modèle fixe (template ou modèle) pour le traitement des plaintes peut favoriser l'objectivité.

En cas de sous-traitance, ces informations doivent, le cas échéant, être demandées à l'officier de sécurité de l'entreprise pour laquelle la personne est employée. Il convient également de l'associer davantage à l'enquête, étant donné que l'officier de sécurité est celui qui est habilité à mener une enquête interne sur les personnes employées dans son organisation.

C. Enquête interne

Un officier de sécurité a le pouvoir de faire une enquête interne afin d'assurer le suivi du screening (art. 13/1 b de la loi du 11/12/1998 relative à la classification et aux habilitations, attestations et avis de sécurité). Dans le cadre d'une enquête interne, il est important de prendre en considération le risque que la personne peut présenter par rapport à l'organisation d'une part, et les informations dont on dispose sur la personne concernée, d'autre part. Les actions à entreprendre et l'enquête sur la personne concernée doivent être proportionnelles au préjudice qu'elle peut causer.

Dès qu'une enquête est en cours, il convient de recueillir naturellement les informations nécessaires pour prendre une décision en connaissance de cause. Plusieurs actions peuvent être entreprises à cet égard :

- Entretien avec la personne concernée et la personne qui a signalé le fait : il est important d'entendre les deux parties ;
- Enregistrement des données relatives aux activités ;
- Des entretiens avec des collègues ;
- Observation de la personne ;
- Vérification source ouverte ;
- …

Cette étude doit être aussi documentée que possible afin de servir de base à d'éventuelles actions. À cet égard, il convient de tenir compte de l'exigence de respect de la vie privée (accès aux informations, conservation de ces informations, ...). L'enquête sera proportionnelle au risque que la personne peut représenter pour l'organisation. Cette enquête interne peut recueillir des données à caractère personnel de la personne, c'est dans l'intérêt général de l'organisation et de la compétence légale de l'officier de sécurité, mais elle doit donc toujours être examinée au regard du principe de proportionnalité.

Les informations recueillies doivent être analysées par les responsables de l'enquête interne afin de déterminer si la personne représente une menace réelle pour l'organisation.

D. Mesures

Au début ou au cours de l'enquête

En fonction du risque que représente la personne pour l'organisation, il peut être décidé de prendre certaines mesures de prévention dès le début de l'enquête :

- Limiter l'accès ;
- Accompagnement supplémentaire ;
- ...

S'il est décidé de prendre de telles mesures, il est préférable de le communiquer clairement à la personne concernée. Il convient de savoir que de telles actions peuvent entrainer une personne à s'éloigner ou de diminuer la confiance d'une personne envers son organisation. Il est donc primordial de soutenir une communication aussi ouverte que possible à cet égard. Il convient alors de parler avec la personne concernée, de sorte que le signalement puisse également être discuté d'un commun accord et que la personne concernée ait la possibilité d'expliquer son point de vue.

Cette décision peut également être prise au cours de l'enquête si, au fil du temps, l'analyse indique que le risque pour l'organisation semble être plus élevé.

La proportionnalité doit être prise en compte lors de la mise en œuvre des opérations. L'adoption de mesures concrètes peut également pousser une personne vers une menace qui n'était pas présente au début.

Une autre option consisterait à demander une analyse supplémentaire à l'Autorité Nationale de Sécurité (ANS) sur base d'informations collectées au préalable.

Après enquête

Une conclusion sera tirée à la fin de l'enquête : existe-t-il une menace potentielle pour laquelle des mesures supplémentaires doivent être prises ? Les actions possibles sont les suivantes :

- Poursuite du suivi ;
- Mesures de sécurité supplémentaires : l'accompagnement, ... ;
- Travailler dans un autre lieu ;
- Suspension ;
- Fin du contrat.

S'il n'y a pas de menace concrète pour l'organisation elle-même, mais que la personne se trouve dans une situation dans laquelle elle peut recourir de l'aide ou du soutien, il convient d'examiner ce que l'organisation peut faire à cet égard. Il s'agit de préserver la confiance de la personne concernée suite à une enquête éventuelle et la remettre sur une voie plus positive.

E. Rapports internes (équipe/interne)

En cas de signalement fondé, la personne concernée peut être informée de l'enquête. Dans la plupart des cas, une conversation sera prévue avec elle. Au moment de l'achèvement de l'enquête interne, un résumé des conclusions doit être communiqué à l'intéressé.

Dans la mesure du possible, le processus de notification peut s'appuyer sur l'existence d'un contact avec l'informateur, sur le fait que tout a été examiné et si des mesures (effectives) ont été prises. Il convient d'être prudent de ne pas transmettre trop de données concernant l'enquête. Cependant, si des mesures effectives ont été prises, cela devra être clair pour tous.

Une communication vers l'équipe de la personne concernée ou les personnes avec lesquelles elle collabore peut également donner des indications sur ce point. En effet, dans ce cas, l'intéressé doit travailler avec des mesures complémentaires. Il faut aussi assurer que l'organisation a toujours confiance en cette personne (étant donné qu'elle est encore employée), mais que des mesures supplémentaires sont prises temporairement pour soutenir la personne et ainsi l'aider à réaliser son travail dans les meilleures circonstances.

À cet égard, il convient de tenir compte du fait qu'une enquête interne, qu'elle soit menée ou non, peut avoir une incidence sur la personne concernée. La confiance dans l'organisation pourrait être compromise par cette personne. Dans ce cas, un suivi plus étroit par le manager pourrait être recommandé. Une communication ouverte au cours du processus, dans le respect nécessaire de la personne concernée, peut y contribuer grandement.

8. Amélioration continue

Ce processus de suivi des employés doit être évalué régulièrement. Le danger de telles mesures est qu'on suppose qu'elles fonctionnent, ce qui peut créer une certaine complaisance dans un système. Il est donc recommandé d'instaurer un cycle d'évaluation permanente à travers lequel ces mesures sont réexaminées de façon continue. On peut notamment évaluer :

- Le succès des mesures (nombre d'enquêtes, de signalements, d'incidents) ;
- La culture de sécurité ;
- Le niveau de soutien des mesures par la direction ;
- L'efficacité de la mise en œuvre de l'approche graduée ;
-...

Il sera alors possible de déterminer si des mesures supplémentaires peuvent être prises ou si des initiatives moins efficaces peuvent être adaptées.

Une telle évaluation offre l'opportunité d'accroître la 'sensibilisation' et de réévaluer le succès du programme de suivi. Il s'agit d'assurer une amélioration continue adaptée à l'évolution de l'organisation.

9. Conclusion

La « menace interne » est une menace réelle pour le secteur nucléaire. Cette menace est entièrement déterminée par les employés de l'organisation et la nature de l'organisation. Il est donc important de surveiller ces personnes avant et pendant l'emploi et après la fin de l'engagement. Dans ce document, nous avons tenté d'implémenter les lignes directrices internationales en la matière à la situation belge avec l'aide des acteurs nationaux. En testant ces éléments avec les personnes travaillant sur le terrain, nous avons pu échanger des bonnes pratiques au sein du secteur, mais aussi avec d'autres secteurs. De toute évidence, il n'existe pas de solution universelle pour le suivi des employés. Les mesures doivent toujours être ciblées sur une organisation spécifique. C'est en partie la raison pour laquelle il a été décidé de dresser un 'aperçu' des différentes mesures possibles. L'installation nucléaire ou le transporteur peut choisir les mesures qui pourraient soutenir sa propre organisation.

ANNEXE A : Signaux qui pourraient indiquer un comportement changeant

Les caractéristiques ci-dessous peuvent indiquer qu'une personne peut être exploitée plus facilement ou qu'elle peut devenir peu fiable. Le fait de présenter l'un des comportements suivants n'indique pas pour autant automatiquement qu'une personne entreprendra une action d'initié, mais cela pourrait l'y conduire plus facilement. En fonction de la situation, ces facteurs peuvent être inquiétants. De plus, le fait qu'une personne présente l'un de ces comportements ne constitue pas forcément un motif d'enquête approfondie, mais si plusieurs éléments remontent, ceci peut être revu d'autant plus lorsque le comportement observé sort des habitudes de la personne. Il s'agit donc d'un aperçu non exhaustif de comportements possibles qui doivent être rapportés :

Présence :
- Quitter le poste de travail sans autorisation (quand une autorisation est requise)
- Abus de jours de maladies de façon répétitive ou pour une longue période sans motif apparent
- Retards fréquents au travail (alors que cela n'était pas une habitude)
- Excuses spécifiques et invraisemblables pour des absences ou des retards
- Absences de courte durée non planifiées et répétées (avec ou sans certificat médical)
- Absence pendant les heures de travail ou difficultés à trouver la personne
- Demandes fréquentes de prendre en charge le travail à sa place.

Productivité :
- Ne respecte pas les deadlines et les engagements de façon répétée sans motif justifié
- N'est pas fiable (par exemple, on ne peut pas se fier à l'endroit où il dit être ou à ce qu'il dit faire)
- Donne des excuses invraisemblables pour des tâches mal exécutées
- Evite de travailler ou ne fait pas tout le travail qui lui incombe
- Le travail requiert plus d'efforts ou plus de temps que prévu
- Fait des erreurs fréquemment, prend de mauvaises décisions ou fait des erreurs de jugement
- Étourdi soudainement et à plusieurs reprises ce qui a un impact sur son travail
- Difficultés à suivre les instructions, incompréhension et manque de volonté de comprendre

Stabilité émotionnelle :
- Hypersensible à la critique
- A du ressentiment et agit en conséquence à l'égard de ses collègues, de son supérieur hiérarchique et/ou de l'organisation
- Sautes d'humeur fréquentes

- Rapidement irrité
- Accès d'agressivité
- Irritabilité accrue avec ses collègues ou d'autres personnes
- Suspicion inhabituelle ou paranoïa
- A l'air anxieux, nerveux ou paniqué
- Exceptionnellement énergique, hilare, euphorique
- A l'air dépressif, exprime un sentiment de désespoir profond vis-à-vis de sa vie ou de son travail ou de la société en général
- Indécis, manque de confiance
- Repli sur soi, s'isole des autres de façon soudaine et sans raison apparente
- Apathie, baisse de motivation
- Distrait par sa situation familiale, financière ou juridique, ou d'autres situations stressantes, difficulté à gérer le stress inhérent à cette situation
- Tendances suicidaires ou tentative de suicide

Comportement non désiré sur le lieu de travail :

- Fréquemment sur la défensive
- Rejette la faute sur les autres pour ses problèmes
- Ment et exagère fréquemment
- Se plaint de ses collègues
- Menace ou intimide ses collègues
- Irritation accrue à l'égard de collègues ou d'autres personnes
- Argumentatif systématiquement pour chaque situation ou contexte
- Langage ou comportement sexuel inapproprié
- Comportement hors contexte ou imprévisible
- Ne se tient pas aux règles de sécurité ou ne suit pas les procédures
- Comportement et exigences déraisonnables à l'égard des autres
- Indication de tromperie, comportement délinquant ou manque de fiabilité

Déclin cognitif :

- Habitudes ou rythme de travail désorganisés
- Distrait, rêvasse fréquemment
- Est facilement distrait, impossible de rester concentré
- Mouvements et temps de réaction ralentis
- Problèmes avec la mémoire à court terme
- Idées ou pensées inhabituelles
- Semble avoir un mauvais jugement des applications
- Ne semble pas se rendre compte qu'il est moins en état de travailler correctement, difficulté à prendre de la distance
- A des difficultés à rester alerte

Déclin physique :

- A l'air fréquemment épuisé
- Détérioration de l'hygiène personnelle

- Plaintes physiques et maladies multiples
- Perte de poids significative
- Semble être faible ou détérioration de la santé
- Problèmes d'ouïe
- Tremblements
- Autres signaux de déclin physique

Signaux d'abus d'alcool ou de drogues :

- A l'air de planer ou d'être saoul au travail
- Problème d'élocution inhabituel, désorientation, ou manque de coordination
- Somnolence ou dormir au bureau
- Cacher de la drogue ou de l'alcool dans la voiture/au travail
- A la capacité de boire une grande quantité d'alcool avec peu d'effets, nécessité d'une consommation fréquente d'alcool
- Heures de travail irrégulières
- Absences consécutives inexpliquées les lundis et/ou les vendredis
- Tentatives répétées et infructueuses de ne pas consommer de drogues ou d'alcool
- Utilisation de drogues ou d'alcool afin de gérer le stress
- Abus de médicaments sous prescription

Signaux indiquant un changement de l'état mental :

- Sautes d'humeurs inexpliquées
- Augmentation de la nervosité ou de l'anxiété
- Diminution des prestations ou des habitudes de travail
- Changement en ce qui concerne l'hygiène personnelle
- Expression de pensées, perceptions ou attentes inhabituelles
- Manque de fiabilité et mensonges
- Tentative de se faire mal, besoin répété de sensations fortes et dangereuses
- Insatisfaction à l'égard de l'employeur ou de l'autorité contractuelle

Non-respect et signaux qui indiquent une possible agression :

- Comportement argumentatif ou abusif à l'égard des collègues de travail ou de la famille, entraînant des discussions sur le lieu de travail ou des interruptions des activités professionnelles.
- Tendance à l'auto-isolement, rejet des interactions sociales, manque de soutien social, dépression inexpliquée et manifeste
- Débordements verbaux, attirant généralement l'attention sur des sujets qui ne sont pas directement liés à la discussion ou au travail.
- Exploitation ou mauvais traitement d'autrui, généralement par intimidation ou abus de pouvoir
- Comportement perturbateur sur lequel les conseils ou la supervision de la direction ne semblent pas avoir d'impact

- Menaces verbales ou physiques à l'encontre de collègues ou de membres de la famille
- Déclarations extrêmes ou répétées exprimant l'amertume, le ressentiment ou la vengeance
- Attaques violentes ou jets d'objets à tout moment
- Comportement de harcèlement
- Violations extrêmes ou récurrentes des règles ou des lois
- Abus en tout genre

Signaux qui indiquent que la personne est active dans le milieu criminel (ou suspicion) :
- Vol ou tentative de vol
- Fraude ou tentative de fraude
- Violence ou négligence à l'égard du conjoint / d'un enfant
- Tentatives d'impliquer d'autres personnes dans des activités illégales ou suspectes

Signaux qui indiquent l'abus d'informations sensibles :
- Faire parvenir des informations à des personnes n'ayant pas accès
- Poser des questions concernant des opérations et/ou des projets auxquels la personne n'a pas ou plus accès
- Contacts non autorisés avec les médias
- Collecte ou stockage de matériel sensible en dehors des installations prévues à cet effet
- Habitudes de sécurité laxistes (traitement d'informations sensibles au téléphone, ne pas faire usage de l'endroit prévu pour le stockage d'informations sensibles, travailler sur des informations sensibles à la maison)
- Déclarations ou actions qui démontrent que la personne pense que les règles ne s'appliquent pas à elle

Signaux qui indiquent l'abus des capacités informatiques :
- Accès à des bases de données sans autorisation ou sans nécessité
- Recherches/navigation non autorisées dans les bibliothèques informatiques
- Suppression non autorisée d'informations sur des bases de données

Signaux qui indiquent une vulnérabilité financière :
- Impossibilité de rembourser des dettes ou plan de médiation de dettes non respecté
- Dépenses compulsives et répétées
- Ne pas assurer correctement le suivi des finances ou des biens de l'organisation

Signaux qui indiquent de la connivence :
- Vivre/dépenser au-delà de ses moyens financiers

- Importantes sommes d'argent inexpliquées ou inattendues
- Remboursements inattendus de dettes
- Déclarations de sommes importantes provenant d'un héritage, de proches fortunés, de cadeaux, d'investissements, d'une entreprise familiale, etc.
- Patrimoine personnel incompatible avec le revenu

Signaux qui indiquent des liens avec des tiers suspects :

- La possession et l'utilisation d'un passeport étranger
- L'encouragement ou la glorification d'actions agressives menées par des tiers ou des organisations
- Association ou sympathie pour des personnes et/ou des organisations qui encouragent ce genre d'actions.

Signaux qui indiquent que la personne a été recrutée :

- Contacter/avoir des contacts avec des personnes connues pour leurs contacts ou leurs éventuels contacts avec des services de renseignement étrangers ou des organisations terroristes.
- Ne pas signaler les voyages à l'étranger
- Ne pas signaler les approches d'organisations étrangères
- Ne pas signaler les demandes d'informations sensibles en dehors des canaux officiels
- Participer ou être invité à participer à des activités illégales

Signaux qui indiquent que la personne récolte des informations ou qu'elle fait disparaitre des matières :

- Questions concernant l'obtention d'informations ou de matières auxquelles la personne n'a pas accès
- Demande de signatures pour confirmation de suppression d'informations ou de matériel sans que vous n'ayez vu la suppression avoir lieu
- Utilisation d'appareillage non autorisé dans des zones ou des informations ou du matériel sensibles sont sauvegardés, discutés ou traités
- Utilisation de matériel d'écoute ou d'observation dans des zones sensibles ou des zones sécurisées
- Transport d'informations ou de matériel sensibles à domicile ou dans d'autres lieux non autorisés
- Accès à des systèmes d'informations numériques sensibles sans autorisation
- Observer un collègue qui essaie d'avoir accès à des informations ou du matériel sensibles qui ne sont pas en rapport avec les tâches professionnelles
- Montrer un intérêt inhabituel pour des informations ne relevant pas du poste de travail actuel
- Intérêt ou aptitudes inhabituelles pour la sécurité
- Jauger délibérément la réaction des services de sécurité

Signaux qui indiquent qu'un collaborateur a des intentions criminelles :

- Essaie d'avoir accès à des zones qui contiennent des informations sensibles en se portant régulièrement volontaire pour des tâches ne relevant pas de ses responsabilités habituelles
- Utilisation excessive des photocopieuses, imprimantes ou autres appareils afin de reproduire ou transmettre des informations qui dépassent les compétences de la personne
- Tentatives d'attirer des collègues dans des situations qui peuvent les mettre dans une position compromettante
- Tentatives d'imposer une obligation à des collègues par un traitement spécial, des faveurs, des cadeaux, de l'argent ou d'autres moyens

Extra info "THE BEHAVIOUR BAROMETER: An Education and Awareness Tool": BAROMETRE_EN_CPRLV_2016-1.pdf (info-radical.org)

ANNEXE B : Lien à la recherche doctorale donnant un aperçu des mesures

Title	**Exploring insider threat awareness and mitigation: more than the devil in disguise**
Author	***Reveraert, Mathias***
Abstract	Employees that steal, commit fraud, sabotage, or leak confidential information: it is every employer's nightmare. Even though every public or private organisation – big or small – is vulnerable to so-called 'insider threats', this problem is too often overlooked because organisations assume that their employees can be trusted. Indeed, employees need to be trusted with access to the organizational assets because they need it in order to do their job. Still, this access implies that insiders are largely exempted from the security obstacles that external enemies have to overcome. Despite the fact that insiders can relatively easier threaten the organization's assets, they are often overlooked as potential threat. Belgium already encountered multiple insider threat incidents. The most striking example is the nuclear reactor Doel 4 that was deliberately sabotaged by an insider. More recent examples in Belgium are Jürgen Conings and Operation Sky. To on the one hand raise awareness on the insider threat problem, and on the other hand provide organizations with mitigation measures to better secure themselves against insider threats, research was done with the support from Brussels Airport Company, Bel-V, Elia, Engie-Electrabel, the Federal Agency for Nuclear Control and G4S on the insider threat problem. The results of the first part of the research provide us with insights on the awareness gaps of Belgian organizations concerning the characteristics of the insider threat as well as the ways to mitigate it. The results of the second part of the research give useful insights on what can be considered 'red flags' of insider threats that organizations should be vigilant of, as well as with mitigation measures that organizations can use to better secure themselves against insider threats.
Language	English
Publication	Antwerpen: Universiteit Antwerpen, Faculteit Sociale Wetenschappen, Departement Politieke Wetenschappen, 2023
Full text (open access)	https://repository.uantwerpen.be/docstore/d:irua:17211

ANNEXE C: Tips & Tricks pour un entretien[5]

When you have a doubt on someone's behaviour or changes in behaviour are noticeable, often the person isn't malicious, and it can be useful to talk to the person themself in order to have an idea of the reason. Information gathering is necessary in order to conduct a threat assessment. Data can be very useful, but to gather information on the intent or motivation, information from the person themself is of the biggest importance.

In general, you will gather more information if you can have an informal conversation (one on one), but it depends on the national legislation and your company culture whether this is possible. In some cases, you may need to have the conversation with a third party present. For example, it can help to have an objective view on what was discussed. In that case, it will be useful to prepare who will lead and who will observe (with a focus on how the person reacts and acts). Sometimes, the interviewed person may ask to have counsellors (advocate, union representatives…) with them.

Preparation of the meeting

°Gather the information you already have. You can use such information during the conversation, for example to substantiate or explain why you ask a question. Be sure to identify facts from assumptions and hearsay.

°During the meeting, you may want to offer support and help to the person: gather information on how you could do it in a concrete way.

°Make sure you know what you want out of the meeting: which information. The objective should be to "clear" the person by finding clear and innocuous explanations for suspicious elements.

°Check what kind of information you are legally authorized to ask. You may refer to regulations regarding private life, medical secrecy, anti-discrimination…

°Prepare (open) questions, to receive the needed information. Open questions may acquire more information.

°Leave your own perception out of your preparation, try to be as objective as possible. It could help to identify what your perception is in order to get it out of the questions/conversation. Try to keep an open mind and approach the meeting with good intent toward the person.

Invitation to the meeting

°Make sure you are in a place where you cannot be disturbed.

°An invitation to a planned meeting can be helpful, so the person cannot pretend to be needed elsewhere – but it might make the person suspicious depends on company culture.

[5] IMPORTANT: These tips & tricks are appropriate for usual situations, when most of the time, people are not dangerous criminals and terrorists and, therefore, must be treated with respect and care. If you have proof or serious doubt on the fact that the person is malicious and/or dangerous, instead, you should contact your security service and police in a timely manner before deciding to carry an interview of the person. It could alert and give him/her an opportunity to commit a malicious act or to flee. It could also hamper a judicial investigation.

°Putting yourself in the position where you need help from the person, might help the conversation: 'Could we have a meeting, because I need your help with something'.

Meeting itself

°Inform the person on why you are having the meeting. You have information that needs to be clarified.

°Ask open questions.

°Talk from an "I" perspective. Avoid "you" sentences that are not perfectly factual or questions, because they can be interpreted as a judgment, and the person can feel threatened, and refuse to answer.

°Leave enough silences, so the person can answer and feels free to speak. Most people also tend to "fill the void" and give more information, even unexpected, when silence is given.

°Focus on the care for wellbeing of the person: 'Is there something we can help you with', 'I am concerned about your wellbeing'.

°Create a relaxing environment, so the person doesn't feel threatened.

°Look at the body language of a person. Try to observe.

°If you have doubt on the fact that the person is lying, you can insist on the fact that it is very important that the person is truthful. Information given may be checked and if it is found that the person has lied, it could have consequences.

°If the person seems distressed, try, and reinsure them that you are here to help them, to clarify the situation and, if needed, find solutions suitable both for them and for the service.

°Respect the person.

°Listen to what is being said and leave enough space for the person to talk. They should be talking more than you.

°Note all important elements. Verify with the person that you have well understood what they said.

After the meeting

°Try to make an objective analysis.

°Write down your initial thoughts, you can analyse them later, but the first impression is often the correct one.

°Check information provided by the person.

°If the person required help or support, act accordingly.

°If needed, contact your security service / the police.

ANNEXE D: Circulaire CP3

Cette circulaire a pour but d'améliorer le service et la gestion optimale des activités internes au sein de la police intégrée et ainsi les rendre plus transparentes. L'objectif est d'élaborer un système de contrôle interne. Cela inclut également la gestion des plaintes.

Circulaire CP3 : Circulaire du 29/03/2011 cp3 relative au 'système du contrôle interne' dans la police intégrée, structurée a deux niveaux (openjustice.be)

ANNEXE E : Exemples de formations

Prévention de radicalisation :

- BeFUS - Preventie van gewelddadig extremisme op https://befus.be/2020/12/25/prevention-des-extremismes-violents/?lang=nl
- Handboek Lokale preventie en veiligheid in België op https://politeia.be/nl/artikels/290193-lokale+preventie+en+veiligheid+in+belgi%C3%AB
- VVSG - Rapport Radicalisering & Polarisatie (Ledenbevraging 2022) op https://www.vvsg.be/Publiek/VVSG%20Rapport%20Ledenbevraging%20Radicalisering%20Polarisering%202022.pdf
- Community Policing and the Prevention of Radicalisation (CoPPRa) - Internationale update 2021 op https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/coppra_en

AFCN

AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

Rue du Marquis 1 bte 6A
1000 Bruxelles • Belgique

www.afcn.fgov.be
pointcontact@fanc.fgov.be
+32(0)2 289 21 11

ÉDITEUR RESPONSABLE
Frank Hardeman

Avril 2024