

CONTRÔLE DES ACCÈS LOGIQUES

COMPTES NON NOMINATIFS

RÈGLES DE SÉCURITÉ

Référence	FT_SSI-REG-CAL_Comptes non nominatifs_V1.4.docx
Clef GED	277579
Version	V1.4
Classification	Restreint
Date	21/06/2017
État	Validé
Auteur(s)	Filière Sécurité des SI
Approbateur(s)	Sylvain Lambert
Validation	Direction de la Maîtrise des Risques

Identification du document		
Référence	Titre du document	
FT_SSI-REG-CAL_Comptes non nominatifs_V1.4.docx	Contrôle des Accès Logiques - Comptes non nominatifs	
Version	État du document	Auteurs
1.4	Final	Filière Sécurité des SI

Classification	
Niveau	Diffusion
Restreint	Le personnel de la DSI de France Travail et à ses tiers formellement autorisés (ayant signé une convention, charte de sécurité, clause de confidentialité)

Mises à jour		
Version	Date	Nature de la modification
0.1	24 Janvier 2008	Création du document
1.2	30 mai 2015	Relecture thématique SSI – groupe de travail filière SSI
1.3	31 août 2016	Mises à jour dans le cadre de la refonte du référentiel initiée en 2016
1.4	27 février 2024	Mise à jour suite changement de marque PE → FT

Relectures et validations				
Version	Relu par	Direction	Date	Statut
1.0	RSSI Mylène Zerbib	DSI	13/01/2009	Validé
1.2	RSSI Sylvain Lambert	DSI	04/09/2015	Validé
1.3	RSSI Sylvain Lambert	DSI	16/06/2017	Validé
1.3	Robert Laupy	DGA-DMR	04/10/2017	Validé

Documents de référence	
Référence	Titre du document
[1] Colibri 196557	Demande de dérogation
[2] Colibri 72624	Contrôle des accès logiques - Utilisateurs
Colibri 277581	Contrôle des accès logiques - Administrateurs
[3] Colibri 162788	Règles de gestion des comptes de service
[4] Colibri 74533	Règles de nommage des composants du SI
[5] Colibri 72643	Classification et protection de l'information

SOMMAIRE

1	PRÉAMBULE	4
1.1	Principes fondateurs de la Politique Générale de Sécurité des SI	4
1.2	Enjeux et objectifs du document.....	4
1.3	Champ d'application	4
2	CONCEPTS GÉNÉRAUX	6
3	RÔLES ET RESPONSABILITÉS.....	8
3.1	Organisation générale du contrôle des accès logiques.....	8
3.2	Définition des responsabilités	10
4	RÈGLES DE SÉCURITÉ.....	12
4.1	Règles spécifiques de contrôle des accès des équipements et applications	12
5	ANNEXES.....	17
5.1	Liste des exigences	17
5.2	Glossaire	18

Règles typographiques

Les termes écrits en vert et soulignés, sont définis dans le glossaire de ce document thématique.

Les règles de la thématique « Contrôle des Accès Logiques – Comptes non nominatifs » sont préfixées par le sigle « **CAL-NNOM-** » et sont numérotées par ordre d'apparition. Elles sont définies dans un encart bleu clair comme figuré ci-dessous :

Définition de la règle

Pour certaines règles, des préconisations, recommandations, commentaires ou des évolutions prévisibles sont détaillés au-dessous de la règle.

Préconisations :

La maîtrise d'œuvre est orientée vers une solution pour couvrir la règle de sécurité.

Recommandations :

L'utilisateur est orienté vers un comportement, un usage, afin de respecter la règle de sécurité.

Commentaires :

Des précisions sont apportées afin d'éclairer la règle énoncée.

1 PRÉAMBULE

1.1 PRINCIPES FONDATEURS DE LA POLITIQUE GÉNÉRALE DE SÉCURITÉ DES SI

Les Systèmes d'Information hébergent de nombreuses données qui revêtent un caractère stratégique et qui constituent un patrimoine essentiel que France Travail a l'obligation de protéger efficacement.

Pour ce faire, la Direction adopte une Politique Générale de Sécurité des SI qui s'inscrit dans le cadre de la politique de gestion des risques ; cette politique protège les informations et leurs traitements ainsi que les ressources hébergées par les Systèmes d'Information de France Travail.

1.2 ENJEUX ET OBJECTIFS DU DOCUMENT

De par les informations sensibles et les données personnelles qui constituent le patrimoine de France Travail, le contrôle des accès logiques est un thème essentiel de la sécurité des SI.

Le présent document définit les règles de sécurité relatives au contrôle des accès logiques pour les comptes non nominatifs.

Ces règles visent à :

- Limiter les risques de compromission des Systèmes d'Information,
- Prévenir les accès non autorisés aux ressources et aux informations.

Ce document se limite aux règles des comptes non nominatifs. Il est complété du socle commun qui incombe à tout utilisateur du système d'information, décrit au sein de la thématique « Contrôle des accès logiques – Utilisateurs » [2].

Si une règle énoncée dans le présent document entre en contradiction avec une règle contenue dans le document cité ci-dessus, la règle du présent document prévaut sur le périmètre des comptes non nominatifs.

1.3 CHAMP D'APPLICATION

Le présent document traite du contrôle des accès aux informations et aux ressources des Systèmes d'Information de France Travail accédées via des comptes non nominatifs, quels que soient leurs localisations géographiques et les moyens utilisés.

Ce document s'adresse aux personnels de la DSI de France Travail et à ses sous-traitants ayant accès à ses Systèmes d'Information via des comptes non nominatifs.

En cas de non-applicabilité d'une des règles du présent document, une procédure de dérogation doit être engagée. Cette demande de dérogation [1] sera transmise au Responsable Sécurité des Systèmes d'Information.

Les règles d'utilisation des données peuvent être dépendantes du niveau de leur classification en termes de confidentialité. La classification utilisée est celle définie dans la thématique « Classification et Protection de l'information » [5].

La règle CLA-10 précise les quatre niveaux de classification de confidentialité des documents :

- **Public** : pour tous les documents électroniques et papier de portée publique diffusable sans restriction,
- **Interne** : pour tous les documents électroniques et papier limités à un usage interne à France Travail et à ses tiers formellement autorisés (ayant signé une convention, charte sécurité, clause de confidentialité, ...),
- **Restreint** : pour tous les documents électroniques et papier réservés à des communautés fermées de personnes,
- **Confidentiel** : pour tous les documents électroniques et papier réservés à des communautés fermées de personnes et réclamant des protections spécifiques dans leur communication et leur manipulation.

2 CONCEPTS GÉNÉRAUX

Le contrôle des accès logiques est exercé lorsqu'un accédant cherche à établir une communication ou une connexion à un système ou une application.

L'accédant peut être une personne, un équipement ou un traitement informatique (système, application...).

Le contrôle des accès logiques comprend obligatoirement :

- Une identification.
- Une authentification.
- Un contrôle des habilitations de l'accédant, en regard des rôles qui lui ont été octroyés.

Compte non nominatif

Compte système

Un compte système est un compte attaché à un processus informatique, et nécessaire au fonctionnement d'un système d'exploitation ou d'un service applicatif. Ce type de compte n'est pas interactif : il permet d'établir des connexions authentifiées entre plusieurs composants systèmes et/ou applicatifs du SI.

Exemple : compte System, parfois appelé « LocalSystem »

Compte générique

Un compte générique peut être un compte technique, un compte applicatif ou un compte de service (pour l'usage d'un service). Il peut être partagé par plusieurs services, applications ou utilisateurs du service en fonction de leurs habilitations ou l'utilisation d'un service.

Exemple : compte Oracle, compte sur un serveur pour effectuer des transferts de fichiers...

Compte de formation

Un compte de formation est un compte utilisé dès lors qu'un accès à un ou plusieurs composants du SI (principalement des applications) est utilisé dans le cadre d'une formation

Exemple : compte de formation pour le SIRH...

Identification

L'identification est l'opération par laquelle un système, un équipement réseau ou une application s'assure qu'il/elle connaît l'accédant qui cherche à se connecter.

Authentification

L'authentification, est l'opération par laquelle un équipement ou un traitement informatique (système, application) vérifie que l'accédant qui souhaite se connecter est bien celui qu'il prétend être.

Cette opération peut s'appuyer sur :

- Une information que l'utilisateur connaît : un secret, un mot de passe...
- Une information que l'accédant possède : un token, une clé, un certificat ...
- Une information qui lui est propre : une empreinte digitale, le son de sa voix...

Rôle

Un rôle est un ensemble de droits attribués à un accédant ; chaque accédant est associé à une liste de rôles.

Un ou plusieurs rôles correspondent à un profil métier.

Les rôles sont définis par les personnes en mesure d'identifier les besoins des accédants et sont généralement construits de manière à refléter une mission ou un métier. Par conséquent, ils peuvent être spécifiques aux entités organisationnelles de France Travail.

Les rôles évoluent au cours du temps et la pertinence des droits regroupés dans un rôle est contrôlée périodiquement.

Habilitation

L'habilitation est l'attribution de droits d'accès à un accédant pour une ou plusieurs ressources des Systèmes d'Information au regard des rôles qui lui sont octroyés.

3 RÔLES ET RESPONSABILITÉS

3.1 ORGANISATION GÉNÉRALE DU CONTRÔLE DES ACCÈS LOGIQUES

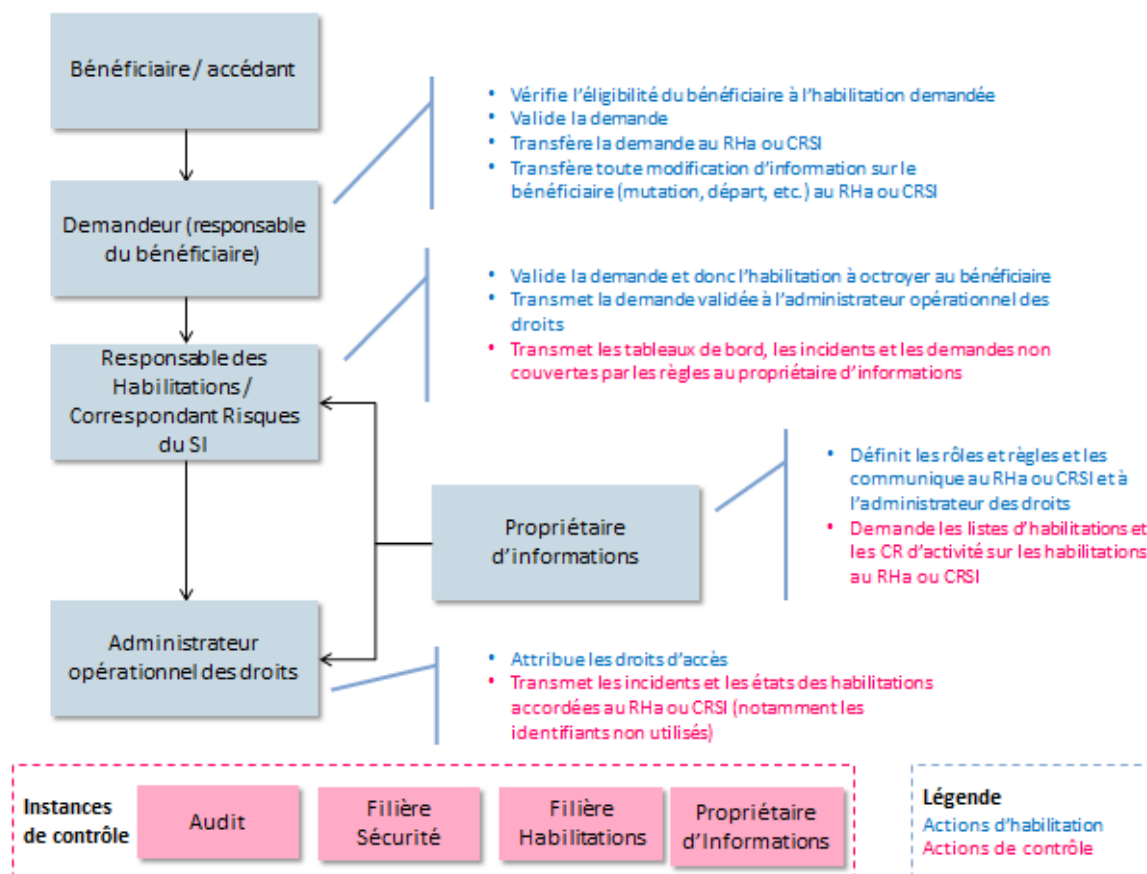
Le contrôle des accès logiques s'appuie sur les trois natures d'instances suivantes :

- **Des instances fonctionnelles** : les résultats et règles décidées sont ensuite validés sous contrôle de la DMR en Comité de Pilotage des habilitations. Elles participent à la définition des rôles, des droits d'accès et des règles d'habilitation sur les SI et les appliquent dans un principe de séparation des pouvoirs (demandeur, signataire, responsable de l'habilitation),
- **Des instances opérationnelles** : déclinées par chaque direction dont la DSI. Elles mettent techniquement en application les rôles, les droits d'accès et les règles d'habilitation sur les Systèmes d'Information de France Travail. Ellesinstancient les couples identifiants / authentifiants et leur attribuent des rôles,
- **Des instances de contrôle**, en charge de veiller au respect des règles de sécurité sous la forme de contrôles ou d'audits (revues d'habilitations), selon l'instance considérée.

Le processus d'habilitation s'appuie sur les fonctions suivantes :

- Le Bénéficiaire de l'habilitation,
- Le Demandeur de l'habilitation,
- Le Responsable du Bénéficiaire/Accédant,
- Le Responsable des Habilitations,
- Le Propriétaire d'Informations,
- L'Administrateur Opérationnel des Droits.

Quels que soient le site où se trouvent le Bénéficiaire/Accédant et l'information accédée, le contrôle des accès logiques s'organise autour du modèle ci-dessous :



Selon les cas de figure, ces fonctions sont jouées par des entités ou des responsables différents de France Travail. La gestion des demandes d'habilitation est déclinée dans différents guides opérationnels.

3.2 DÉFINITION DES RESPONSABILITÉS

Les rôles et responsabilités de ces fonctions sont précisés ci-dessous.

Propriétaire d'Informations

Le Propriétaire d'Informations classe les informations dont il a la charge. Il révisé régulièrement cette classification.

Il exprime ses exigences fonctionnelles sur les accès logiques à ses informations.

Il définit notamment les rôles et les règles de gestion des habilitations aux informations. Il les révisé à l'occasion d'évolutions des applications supportant ces informations. Il communique ces rôles et règles aux Administrateurs Opérationnels des Droits et aux Responsables des Habilitations.

Le Propriétaire d'Informations dispose des prérogatives nécessaires pour contrôler la bonne mise en application des règles qu'il a définies. Dans le cadre de ces contrôles, il peut disposer des listes des habilitations et plus généralement des comptes rendus des activités liées aux habilitations.

Bénéficiaire/Accédant

Le Bénéficiaire/Accédant peut être un utilisateur, un exploitant, un acteur d'un projet, une application...

Responsable du Bénéficiaire/Accédant

Le Responsable du Bénéficiaire/Accédant renseigne et signe la demande d'habilitation du Bénéficiaire/Accédant.

Cette signature a un double objectif : d'une part, garantir l'identité du Bénéficiaire/Accédant, d'autre part, permettre au Responsable des Habilitations de vérifier que le Bénéficiaire/Accédant est bien éligible à l'habilitation demandée.

Il s'assure que les besoins exprimés sont cohérents avec l'activité du Bénéficiaire/Accédant. Il signale au Responsable des Habilitations toute évolution relative au statut du Bénéficiaire/Accédant (mutation ou départ de l'utilisateur, application retirée de la production...).

Responsable des Habilitations

Le Responsable des Habilitations valide la demande d'habilitation :

- Il s'assure que la demande est dûment renseignée et signée.
- Il contrôle les besoins d'habilitation du Bénéficiaire/Accédant et lui associe le(s) seul(s) rôle(s) nécessaires(s) d'habilitation sur les Systèmes d'Information.
- Il argumente les refus d'habilitation en s'appuyant sur les règles définies par les Propriétaires d'Informations et sa connaissance des Métiers.

Il la transmet alors à l'Administrateur Opérationnel des Droits.

Le Responsable des Habilitations remonte, sur demande des Propriétaires des Informations accédées:

- Le tableau de bord nécessaire au suivi des habilitations,
- Tout incident relatif aux habilitations qui les concerne,
- Toute demande non couverte par les règles de gestion des habilitations.

Administrateur Opérationnel des Droits

L'Administrateur Opérationnel des Droits met en application les règles et rôles de contrôle des accès logiques. Il attribue les droits.

Il traite, dans les délais précisés par les Propriétaires d'Informations, les demandes transmises par les Responsables des Habilitations.

Il délivre les états des habilitations accordées (notamment la liste des couples identifiants/authentifiants inutilisés) aux Responsables des Habilitations et leur remonte tout incident.

Mensuellement, il remonte un historique du traitement des demandes d'habilitations par direction / région (état du stock de demandes au mois M, état du stock de demandes au mois M+1, nombre de demandes, % de demandes traitées dans les délais,...).

4 RÈGLES DE SÉCURITÉ

4.1 RÈGLES SPÉCIFIQUES DE CONTRÔLE DES ACCÈS DES ÉQUIPEMENTS ET APPLICATIONS

CAL-NNOM-01 Comptes non nominatifs

À titre exceptionnel, certaines populations doivent partager la connaissance de couples identifiant/authentifiant. Ces populations doivent prendre toutes les mesures nécessaires pour assurer la confidentialité de ces couples.

Cette règle concerne également les équipements et les traitements informatiques. En cas de partage exceptionnel de couples identifiant/authentifiant, les mesures suivantes -non exhaustives- peuvent être appliquées selon les situations et moyens à disposition:

- Le couple identifiant/authentifiant est modifié au départ d'un des membres de l'équipe partageant le compte non nominatif,
- L'authentifiant est chiffré *****,
- Etc...

Ces comptes non nominatifs sont sous la responsabilité du responsable de l'activité qui a besoin d'utiliser ce type de compte. Le correspondant sécurité de la direction doit être associé à la demande.

Les comptes systèmes ne doivent pas être interactifs, et les données d'authentification (si existantes) ne sont pas communiquées. La source de connexion doit être connue et maîtrisée.

Commentaires

Les comptes génériques et les comptes de formation ont des besoins spécifiques liés à l'authentification en fonction de cas d'usages, comme par exemple, la mise en veille désactivée, un autologon, etc...

Toutes ces règles de gestion sont définies dans les documents cités ci-après :

- [3] Règles de gestion des comptes de service,
- [4] Règles de nommage des composants du SI.

CAL-NNOM-02 Responsabilité d'usage de comptes non nominatifs

Un responsable doit être formellement désigné pour toute demande de compte non nominatif

CAL-NNOM-03 Gestion des comptes génériques

Les « comptes constructeurs », « comptes par défaut » ou « comptes d'usine » doivent être considérés comme des comptes à privilèges. Ils donnent souvent des accès privilégiés à certains systèmes ou équipements.

Les comptes d'installation et comptes par défaut sont supprimés ou désactivés dès que possible.

Dans le cas contraire, les authentifiants des équipements ou applications doivent être systématiquement modifiés par les équipes opérationnelles (Administration & Exploitation) avant leur mise en production.

Commentaires

Plus particulièrement, les mots de passe par défaut des constructeurs et éditeurs doivent être changés.

La construction des authentifiants des comptes génériques doit se conformer à la règle «Construction des authentifiants des comptes systèmes et comptes génériques» décrite dans cette thématique.

CAL-NNOM-04 Utilisation de comptes systèmes

De manière générale, les comptes systèmes ne permettent pas de connexion au système pour un utilisateur (personne physique) : ces comptes sont réservés aux connexions inter applicatives.

Dans le cas où une connexion avec ce type de compte serait nécessaire (maintenance, exploitation), la source de connexion doit être connue et maîtrisée.

CAL-NNOM-05 Utilisation de comptes génériques

Les serveurs comportant des comptes génériques (compte «root», compte «applicatif», etc..) doivent être protégés de l'utilisation directe de ces comptes depuis un poste de travail.

Dans le cas où une connexion avec ce type de compte serait nécessaire, la source de connexion doit être connue et maîtrisée.

Commentaires

L'usage du compte générique «compte de service» est réservé à un poste de travail ou un groupe de postes de travail identifié (plages d'adresses IP réservées). Il n'a pas vocation à se connecter sur un poste de travail utilisateur.

CAL-NNOM-06 Utilisation de comptes de formation

Les comptes de formation ne doivent pas avoir accès aux données de production.

CAL-NNOM-07 Comptes de contrôle et d'audit

Dans le cadre d'opérations de contrôle et d'audit (Commissaires aux Comptes, audit sécurité, audit interne, contrôle interne), l'usage de comptes d'audit et de contrôle est possible et est réservé à des personnes dûment habilitées.

Les comptes sont activés pour la période d'audit ou de contrôle identifiée et désactivés en dehors de celle-ci.
Ce compte de contrôle et d'audit est sous la responsabilité de l'équipe de contrôle / d'audit l'ayant sollicité.

Commentaires

La traçabilité doit permettre sur une période de un an d'identifier à quelle personne physique est rattaché l'identifiant banalisé et sur quelle période précise.

CAL-NNOM-08 Référentiel des comptes non nominatifs

Un référentiel des comptes non nominatifs doit être mis en place et maintenu à jour.

CAL-NNOM-09 Construction des authentifiants des comptes systèmes et génériques

Lorsque l'authentifiant est un mot de passe, il doit être choisi de manière à n'être ni évident, ni prévisible. Le mot de passe utilisé doit être robuste (non vulnérable à des tentatives d'accès frauduleux).

La construction de l'authentifiant « mot de passe » doit obéir aux critères de qualité suivants :

- Avoir une longueur minimale de **quinze** caractères
- Être composé de caractères appartenant aux trois classes suivantes : lettres (a...z et A...Z), chiffres (0...9) et caractères spéciaux (&@à(|...)
- Être différent au moins des **deux** mots de passe précédents.

Les responsables des comptes non nominatifs doivent être sensibilisés à ces modalités de construction. Les correspondants Sécurité, identifiés au sein de France Travail ont, par ailleurs, légitimité pour en vérifier l'application. À l'occasion de telles vérifications, ils réclament aux responsables des comptes non nominatifs le changement sans délai de leur authentifiant « mot de passe » dévoilé.

Les responsables de ces comptes s'engagent à respecter ces règles et procédures de contrôle.

Commentaires

Si possible, l'usage d'une authentification basée sur une clé cryptographique est à privilégier, assurant ainsi la sécurisation de la méthode d'accès.

Pour les comptes de formation, la construction des authentifiants doit être à minima conforme à la règle de construction des authentifiants définie dans le document chapeau «Contrôle des Accès Logiques – Utilisateurs» [2].

CAL-NNOM-10 Révision des authentifiants des comptes non nominatifs

Les authentifiants « mots de passe » doivent pouvoir être changés sur demande.

CAL-NNOM-11 Prévention contre les attaques de type « force brute »

Afin de se prémunir des attaques de type « force brute », un mécanisme de blocage du compte doit être mis en place. Ce mécanisme doit être adapté au contexte et permettre d'empêcher les tentatives répétées de connexions.

5 Annexes

5.1 LISTE DES EXIGENCES

CAL-NNOM-01	Comptes non nominatifs	12
CAL-NNOM-02	Responsabilité d'usage de comptes non nominatifs.....	12
CAL-NNOM-03	Gestion des comptes génériques	13
CAL-NNOM-04	Utilisation de comptes systèmes.....	13
CAL-NNOM-05	Utilisation de comptes génériques	13
CAL-NNOM-06	Utilisation de comptes de formation.....	13
CAL-NNOM-07	Comptes de contrôle et d'audit	14
CAL-NNOM-08	Référentiel des comptes non nominatifs.....	14
CAL-NNOM-09	Construction des authentifiants des comptes systèmes et génériques	14
CAL-NNOM-10	Révision des authentifiants des comptes non nominatifs	16
CAL-NNOM-11	Prévention contre les attaques de type « force brute »	16

5.2 GLOSSAIRE

Authentification

L'authentification est l'opération par laquelle un équipement ou un traitement informatique (système, application) vérifie que l'utilisateur qui souhaite se connecter est bien celui qu'il prétend être.

Une authentification forte est définie comme requérant deux éléments :

Authentification forte

- Quelque chose que l'utilisateur possède (une carte à puce, un token qui génère un code automatique à durée de vie limitée),
- Un secret que l'utilisateur connaît et qui n'est pas partagé par d'autres personnes (un mot de passe, un pin code, etc....).

Critique

La classification des informations repose sur la notion suivante : le propriétaire d'informations classe ses informations et définit leur niveau de sensibilité (non sensible, Sensible, Critique, Stratégique) duquel est déduit le niveau de protection et de service à mettre en œuvre.

Habilitation

L'habilitation est l'attribution de droits d'accès à un utilisateur à une ou plusieurs ressources des Systèmes d'Information.

Identification

L'identification est l'opération par laquelle un système, un équipement réseau ou une application s'assure qu'il/elle connaît l'utilisateur qui cherche à se connecter.

Privilège

Il s'agit d'un ensemble de droits accordés sur un système, permettant d'effectuer des actions sur celui-ci (création, consultation, modification, suppression).

Ressource

Le terme 'ressource' regroupe tout élément des SI participant au stockage, transport ou traitement de l'information. Il peut s'agir de matériel, logiciel, procédure de traitement, ressources humaines, organisation

Rôle

Un rôle est un ensemble de droits attribués à un accédant et chaque accédant est associé à une liste de rôles.

RSSI

Responsable de la Sécurité des Systèmes d'Information.

Sensible

La classification des informations repose sur la notion suivante : le propriétaire d'informations classe ses informations et définit leur niveau de sensibilité (non sensible, Sensible, Critique, Stratégique) duquel est déduit le niveau de protection et de service à mettre en œuvre.

Stratégique

La classification des informations repose sur la notion suivante : le propriétaire d'informations classe ses informations et définit leur niveau de sensibilité (non sensible, Sensible, Critique, Stratégique) duquel est déduit le niveau de protection et de service à mettre en œuvre.

Token

Token est le mot anglais pour jeton. Le token se présente sous la forme d'une petite calculatrice et génère un code automatique à durée de vie limitée : un mot de passe à usage unique. Le token est donc un moyen d'authentification forte.

Tiers

Le terme désigne l'ensemble des prestataires et des intérimaires employés à titre individuel et amenés à accéder aux informations ou ressources de France Travail.

Utilisateur

Le terme désigne l'ensemble des personnes susceptibles de pouvoir accéder aux SI de France Travail.

(Fin de document)