

SUPPORT ET EXPLOITATION

RÈGLES DE SÉCURITÉ

Référence	FT_SSI-SEE_Support et Exploitation_v1.2.docx
Clef GED	72647
Version	V1.2
Classification	Interne
Date	17/06/2020
État	Final
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-SEE_Support et Exploitation_v1.2.docx	Support et Exploitation	
Version	État du document	Auteurs
1.2	Final	Filière Sécurité des SI

Classification

Niveau	Diffusion
Interne	Le personnel 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
1.0	10 Juin 2009	Validation DGA-QMR
1.1	16/06/2020	Mises à jour dans le cadre de la directive NIS (conformité OSE)
1.2	20/02/2024	Mise à jour suite à changement de marque PE→FT

Relectures et validations

Version	Relu par	Direction	Date	Statut
1.0	COPIL SSI	DGA-SI	13/01/2009	Validé
1.0		DGA-QMR	10/06/2009	Validé
1.1	RSSI Sylvain Lambert	DSI	17/06/2020	Validé

Documents de référence

Référence	Titre du document
[1] Colibri 196557	Demande de dérogation
https://www.ssi.gouv.fr/uploads/2015/02/guide_admin_securisee_si_anssi_pa_022_v2.pdf	Guide Admin sécurisé de l'ANSSI

SOMMAIRE

1. PRÉAMBULE	5
1.1. Principes fondateurs de la Politique Générale de Sécurité des SI	5
1.2. Enjeux et objectifs du document	5
1.3. Champ d'application	5
2. RÔLES ET RESPONSABILITÉS	6
3. RÈGLES DE SÉCURITÉ	7
3.1. Support	7
3.2. Exploitation	9
3.2.1. Dispositions générales	9
3.2.2. Gestion des médias	13
3.2.3. Sécurité physique	15
3.2.4. Gestion des changements	17
3.2.5. Reporting / tableaux de bord	18
4. ANNEXE	20
4.1. Glossaire	20
4.2. Liste des règles	22

Règles typographiques

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

Les règles thématiques sont préfixées par le sigle « **SEE-** » 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

Les fonctions de support et d'exploitation ont en charge la mise en œuvre et le maintien des solutions de sécurité garantes de la protection des Systèmes d'Information. De par leurs missions et les privilèges importants qu'elles confèrent aux exploitants et administrateurs, ces fonctions doivent être une préoccupation permanente de la sécurité des Systèmes d'Information.

Le présent document a pour objectif de garantir le niveau de sécurité des Systèmes d'Information par une homogénéisation des solutions mises en œuvre et un encadrement strict des opérations de support et d'exploitation.

1.3. CHAMP D'APPLICATION

Le présent document concerne l'ensemble des équipements de France Travail et s'adresse tout particulièrement aux équipes en charge du Support, de l'Administration et de l'Exploitation des équipements (équipements réseaux, postes de travail, serveurs, équipements de sécurité, messagerie, Intranet, accès au réseau Internet, interconnexions avec les tiers).

Les règles sont présentées selon les deux axes suivants :

- Les règles de support qui visent à encadrer les opérations de support tant sur les postes de travail des utilisateurs finaux que sur les serveurs de production,
- Les règles d'exploitation qui sont relatives à la production informatique et aux opérations s'y rattachant (gestion de parc, tableaux de bord, changement,...).

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.

2. RÔLES ET RESPONSABILITÉS

Le présent chapitre a pour but de définir les fonctions intervenant dans les processus de définition, d'application et de contrôle des règles de sécurité concernant le support et l'exploitation. Ces fonctions regroupent des missions et des responsabilités qui correspondent à un ou plusieurs acteurs, directions, au sein de France Travail.

- La Maîtrise d'Ouvrage Sécurité
 - ▶ Définit les exigences de sécurité fonctionnelle,
 - ▶ Participe à la validation des dispositifs de sécurité,
 - ▶ Commandite des contrôles de conformité sur leur mise en place.
- La Maîtrise d'Œuvre
 - ▶ Effectue les opérations de support aux Exploitants.
- L'Administration et l'Exploitation
 - ▶ Déploient, administrent et maintiennent les infrastructures techniques dans un état intègre et opérationnel,
 - ▶ Conduisent la gestion de parc,
 - ▶ Assurent la mise en place des mesures de sécurité,
 - ▶ Maintiennent le niveau de sécurité des infrastructures techniques.
- Les Utilisateurs et Métiers
 - ▶ Respectent les règles de sécurité qui les concernent, notamment les règles de sécurité sur l'utilisation des Systèmes d'Information et de Communication de France Travail.

3. RÈGLES DE SÉCURITÉ

3.1. SUPPORT

SEE-01. Responsabilité des équipes de support

Toute session ouverte lors d'une opération de support doit être fermée une fois l'intervention terminée (session de prise de main à distance, ouverture d'une session avec des droits d'administrateur...).

Seules des personnes habilitées et formées à ces opérations peuvent conduire une opération de support.

Les niveaux d'habilitation des conseillers support diffèrent suivant le niveau de support couvert. Les équipes de support disposent pour leurs activités récurrentes d'un niveau d'habilitation standard ; Ce niveau peut bénéficier d'une extension ponctuelle de privilèges (limitée dans le temps), sur autorisation du responsable d'équipe support, dans le cas d'une intervention spécifique.

Commentaires

Lors d'une opération de support certains éléments doivent être préalablement vérifiés, notamment l'activation de l'antivirus, la version du moteur et la version de la base de signatures.

Le cas échéant, une mise en conformité doit être réalisée dans le cadre de l'opération de support

SEE-02. Contrôle des opérations de support

Toutes les opérations de support doivent être réalisées après une phase d'authentification basée sur un couple identifiant/authentifiant nominatif.

Quand un S.I. traite d'une information de niveau supérieur à 2, un système de traçabilité doit être mis en place.

Dans le cas spécifique du support à l'utilisateur (prise de main à distance sur un poste de travail), les opérations de support ne doivent se faire que sur sollicitation de l'utilisateur et conformément aux règles thématiques applicables aux Postes de Travail.

Pour toute intervention, les informations nécessaires sont tracées de manière à ce qu'il soit possible d'identifier a posteriori au minimum : l'intervenant, l'équipement concerné, les dates et heures de début et de fin d'intervention.

Commentaires

Les fonctions de support, notamment au travers des mécanismes de prise de contrôle à distance des postes de travail des utilisateurs, sont des opérations sensibles qui doivent être encadrées afin d'éviter toute dérive de sécurité.

En effet, les opérations de support par la prise de main à distance, par exemple, se font sous les comptes des utilisateurs et seule la traçabilité permet d'imputer la responsabilité des opérations réalisées.

Les moyens de contrôle permettent de détecter les éventuelles anomalies dans les opérations de support (abus de privilège, session anormalement longue...).

3.2. EXPLOITATION

3.2.1. Dispositions générales

SEE-03. Responsabilité des Administrateurs et des Exploitants

Les Administrateurs et Exploitants des Systèmes d'Information sont tenus d'observer strictement les règles de sécurité et les limites fixées à leurs interventions.

Ils n'abusent pas de leurs privilèges et limitent leurs actions aux ressources informatiques dont ils ont la charge, dans le respect de la finalité de leur mission. En aucun cas, ils ne contournent les procédures de sécurité établies.

Commentaires

Les Administrateurs et Exploitants des Systèmes d'Information sont soumis à une obligation de discrétion liée à leurs activités. Ils ne prennent pas connaissance des données personnelles des utilisateurs, ils respectent la confidentialité des informations auxquelles ils ont accès, ils ne se connectent pas et ne donnent pas accès à des ressources sans y avoir été autorisés.

Ponctuellement, ils peuvent être amenés à prendre connaissance des données personnelles des utilisateurs, sur demande formelle de l'utilisateur. Ils n'autorisent quiconque à y accéder, sauf cas particuliers prévus par la loi (une enquête judiciaire par exemple).

SEE-04. Administration et exploitation des composants des SI

Les équipements d'administration et d'exploitation des composants des SI de France Travail sont des éléments sensibles et doivent être protégés en conséquence.

Les équipes de télé-exploitation appliquent les mêmes directives et consignes que les équipes de production internes.

Les opérations de télé-exploitation depuis un réseau extérieur doivent être réalisées via les infrastructures communes d'accès aux serveurs conformément aux règles thématiques concernant les « Réseaux informatiques ».

Commentaires

Les équipements d'administration et d'exploitation couvrent notamment les consoles déportées et les postes de travail : leur sécurité doit être durcie.

Pour les SIE identifiés dans le cadre du statut d'Opérateur de Services Essentiels, seuls les services et les fonctionnalités qui sont indispensables à leur fonctionnement ou à leur sécurité doivent y être installés. Ceux qui ne le sont pas doivent être désactivés (lorsque la désinstallation n'est pas possible, le mentionner dans le dossier d'homologation du SIE concerné en précisant les services et fonctionnalités concernés et les mesures de réduction du risque mises en œuvre).

En fonction des faisabilités, la protection de ces équipements doit être physique et/ou logique : à titre d'illustration, les contrôles à effectuer peuvent se faire via une authentification renforcée et une journalisation.

La télé-exploitation depuis le réseau externe désigne aussi bien l'exploitation à distance par un agent de France Travail en situation de nomadisme que les opérations d'exploitation à distance faites par des tiers.

Le document thématique concernant les « Réseaux informatiques » interdit par exemple les accès directs par modem. En termes d'infrastructure, les opérations de télé-exploitation sont gérées au niveau des Points d'Accès Externe.

SEE-05. Administration et exploitation des composants d'un SIE

L'ensemble des actions d'administration et d'exploitation des composants du SIE est effectué depuis une ressource physique dédiée.

Préconisations

Les solutions suivantes peuvent être retenues :

- 2 postes de travail séparés pour les actions d'administration et pour la « bureautique » ;
- 1 poste de travail ;
 - ▶ Dédié à l'administration et accédant à une infrastructure de poste de travail virtuel pour la bureautique ;
 - ▶ Avec un dual-boot maintenant une étanchéité entre les deux boots.

SEE-06. Contractualisation des exigences pour les tiers

La délégation des opérations d'exploitation à un tiers doit faire l'objet de spécifications du niveau de sécurité requis. Ainsi, toute externalisation de fonctions ou de services du SI nécessite une analyse de risque au préalable. Selon le périmètre et la sensibilité de la demande, les exigences doivent être exprimées par la Maîtrise d'Ouvrage Sécurité et déclinées en spécifications par la Maîtrise d'Ouvrage Architecture. Elles disposent chacune des droits de contrôle du respect de ces exigences.

Les engagements du tiers vis-à-vis des spécifications doivent être contractualisés.

Les opérations d'exploitation par un tiers ne doivent se faire qu'après accord de l'Administrateur / Exploitant en charge de la ressource. Les résultats sont soumis à sa validation.

Commentaires

Des mécanismes de sécurité complémentaires sont susceptibles d'être exigés au cas par cas, en fonction des garanties en termes de sécurité apportées par la société externe et des besoins en termes d'ouverture de flux.

En cas de besoin de télémaintenance sur un système hébergeant des informations sensibles, la procédure d'accès et de contrôle des actions doit être soumise préalablement au RSSI.

SEE-07. Opérations d'infogérance externe ou de sous-traitance

Dans le cadre d'infogérance ou de sous-traitance de tout ou partie de l'exploitation des SI, il est nécessaire de conserver en interne :

- les compétences nécessaires à la gouvernance des opérations d'exploitation (pouvoir décisionnel, gestion de crise, fonction de contrôle et d'audit, etc.),
- la maîtrise de l'architecture de sécurité des Systèmes d'Information,
- la maîtrise du processus d'attribution de droits aux profils et d'attribution de profils aux utilisateurs.

Les opérations doivent être placées sous le contrôle de la direction du domaine Opérations et doivent faire l'objet d'indicateurs de sécurité.

SEE-08. Gestion de parc

Tout serveur, poste de travail ou application appartenant à France Travail doit être inventorié.

La procédure de gestion de parc doit être claire, accessible et diffusée à tous les exploitants.

Tout changement de configuration ou d'affectation d'un matériel ou logiciel doit être connu et maîtrisé par les Exploitants. Lors du changement d'affectation d'un équipement informatique, il doit être récupéré par l'entité en charge de son administration. Toute information stockée sur cet équipement est alors détruite.

Dans le cas spécifique des postes de travail, la destruction des informations n'est pas

systématique et se fait selon les documents des thématiques « environnement de Travail ».

Commentaires

Les éléments concernés par la destruction sont l'ensemble des supports de stockage (comme par exemple les disques durs, les bandes magnétiques, les disques ou cassettes amovibles, les supports de stockage optique).

Une clause permettant la mise en œuvre de cette exigence de destruction dans le cas d'une mise au rebut doit être prévue dans les contrats de maintenance par les signataires du contrat.

SEE-09. Traçage des mouvements de matériels

Les mouvements des matériels doivent être tracés avec enregistrement des dates de sortie et de retour dans les locaux d'origine, sauf dans le cas d'une autorisation longue durée pour le matériel mobile (ex. postes portables).

SEE-10. Modification de configuration d'un équipement

Quel que soit l'équipement, le mot de passe par défaut doit être modifié.

En cas de réutilisation de l'équipement dans un contexte différent, la réinstallation entière de l'équipement est indispensable.

3.2.2. Gestion des médias

SEE-11. Procédures de gestion des médias

Toutes les procédures relatives à la gestion des médias doivent être formalisées et mises en œuvre de façon à garantir, à tout moment du cycle de vie, des niveaux de sécurité conformes à ceux définis par les Propriétaires d'Information.

Les procédures relatives aux supports contenant des informations sensibles doivent être validées par la MOA Sécurité et publiées.

Commentaires

Ces procédures couvrent notamment :

- les mesures de protection appropriées selon les niveaux de classification des informations contenues dans ces supports (stockage, chiffrement, signature électronique, etc....),
- l'effacement et la destruction des médias (la traçabilité de ces opérations, etc....),
- le convoyage et l'expédition de médias,
- etc.

SEE-12. Protection et stockage des médias

Les supports de sauvegarde doivent être protégés des risques d'altération, de destruction, de divulgation et de vol. Ils doivent être stockés dans les zones de sécurité (cf. règle SEE-16) correspondant à la sensibilité des données qu'ils hébergent.

En conséquence, les supports de sauvegarde doivent être stockés dans des éléments et/ou locaux adaptés, sécurisés et prévus à cet effet (bureaux, armoires, armoires fortes,...). L'accès à ces éléments et/ou locaux doit être géré, au sein de chaque équipe concernée, selon des procédures formelles (gestion des clés, main courante,...).

Quel que soit le lieu de stockage de ces supports, l'expédition doit être opérée avec un dispositif en conformité avec le niveau de sensibilité des données concernées.

SEE-13. Externalisation du stockage des médias

Lorsque le stockage des médias est externe au site, un contrôle préalable des bonnes conditions de stockage doit être effectué et formalisé contractuellement.

SEE-14. Gestion des sorties des médias

Toute sortie de média en dehors des locaux doit être soumise à autorisation.

Elle doit être tracée avec conservation des éléments suivants : date de sortie, identité de l'expéditeur, identité du destinataire, objet, date de retour effectif du support, moyen de convoyage utilisé (service postal, société spécialisée,...).

Ce traçage permet de garantir un suivi du média concerné.

SEE-15. Effacement des médias avant réutilisation

Le contenu de tout média doit être effacé et les données détruites lorsque celui-ci est transmis pour réutilisation à un service n'ayant pas à connaître les informations enregistrées

SEE-16. Vérification des médias d'archivage

L'intégrité et la disponibilité des informations stockées sur les médias d'archivage doivent être contrôlées régulièrement. Elles doivent faire l'objet d'un rapport de contrôle permettant de suivre le cycle de vie des médias.

3.2.3. Sécurité physique

SEE-17. Sécurité des locaux

Tout matériel informatique (serveur informatique, équipement réseau et télécoms...) doit être situé dans une zone protégée conformément à son niveau d'exigence de sécurité.

Chaque local hébergeant des ressources informatiques doit être classifié selon l'une des zones de sécurité suivantes :

- Zones de sécurité **rouges**

Il s'agit de zones de « haute sécurité », de type « salle de production informatique », garantissant un niveau de sécurité maximal en matière de protection physique contre les sinistres et de maîtrise des accès physiques. Ces zones abritent des informations ou des équipements particulièrement sensibles d'un point de vue de la sécurité (pare-feu...). Ces zones sont dites mortes car, en régime normal, elles ne font normalement pas l'objet d'accès réguliers par des personnes physiques.

- Zones de sécurité **oranges**

Il s'agit de zones telles que des locaux « techniques » (routeurs...) ou des locaux d'hébergement d'équipements sensibles (salle de pilotage...), bénéficiant de mesures et moyens de prévention et de protection de risques physiques, conformes à leur usage. L'accès physique à ces zones dites mortes est restreint à une liste maîtrisée de personnes habilitées.

- Zones de sécurité **vertes**

Il s'agit de zones pour lesquelles un contrôle d'accès est requis car elles contiennent des informations ou ressources informatiques sensibles. Ces zones sont dites vivantes car des accès fréquents de personnes physiques sont admis (il s'agit principalement des bureaux de France Travail).

- Zones de sécurité **blanches**

Il s'agit de zones pour lesquelles aucune mesure de contrôle spécifique n'est exigée car elles ne contiennent pas d'informations ou de ressources sensibles. Ces zones sont dites vivantes car des accès fréquents de personnes physiques sont admis, notamment la partie publique d'un France Travail.

Un responsable de la sécurité physique doit être nommément désigné pour chaque zone. Ce responsable est en charge de la mise en œuvre et du contrôle des moyens de prévention et de protection des zones dont il est responsable.

SEE-18. Protection des zones

Chaque zone doit être définie, dimensionnée et protégée en fonction du niveau de sensibilité des informations et ressources qu'elle héberge. La protection peut notamment se faire en termes de :

- Contrôle physique des accès : à titre d'exemple, badge d'accès contrôlé, badge spécifique aux visiteurs ou interdiction absolue des visiteurs, installations de surveillance...
- Menaces internes, externes et environnementales : normes de construction et d'équipement en matière de prévention et de lutte contre les incendies, dégâts des eaux... mais aussi contre les intrusions physiques.
- Moyens généraux d'alimentation électrique : protection contre la foudre, maintien de l'alimentation des équipements en cas de coupures de courant ou de travaux sur les installations principales...
- Sécurisation des câblages : protection contre tout accès malveillant pouvant conduire à des risques d'écoute, d'intrusion ou de déni de service, séparation des câbles par type pour éviter les interférences électromagnétiques...

Commentaires

Les zones mises sous vidéo surveillance sont identifiées conformément à la loi.

SEE-19. Protection des équipements d'administration des accès physiques

Les équipements d'administration et de surveillance des accès physiques (caméras, contrôleurs de badge...) peuvent être connectés au réseau interne.

Dans ce cas, les équipements et logiciels doivent respecter les règles de sécurité du référentiel SSI. Les accès réseau doivent être conformes aux règles définies dans les documents thématiques « Exigences de sécurité appliquées aux tiers » et « Réseaux informatiques ».

Au cas où les équipements ne sont pas connectés au réseau interne, il est toléré qu'ils soient accessibles depuis l'extérieur via une connexion modem, ADSL, etc.

Commentaires

Ces équipements peuvent être configurés de manière à remonter toute anomalie (porte ouverte sur une longue durée, tentatives d'accès incorrectes...).

3.2.4. Gestion des changements

SEE-20. Changement

Toute mesure prise dans le cadre d'un changement doit garantir la possibilité de revenir à la configuration initiale en cas de dysfonctionnement.

Le niveau de sécurité global après l'intervention doit être au moins égal au niveau de sécurité avant l'intervention.

Dans le cadre d'une intervention de maintenance, la sortie de supports contenant ou pouvant contenir des informations sensibles doit être contrôlée et tracée.

Les privilèges accordés au mainteneur doivent être strictement limités à ceux nécessaires pour l'exercice de sa mission.

Commentaires

Le responsable d'un changement est tenu d'avertir les entités utilisatrices des impacts de l'opération de changement sur la disponibilité de l'application, du système ou de la composante des Systèmes d'Information. Les contraintes éventuelles sur l'organisation ou sur les méthodes de travail doivent par la suite être communiquées aux utilisateurs finaux.

SEE-21. Installation des correctifs

L'installation des correctifs requiert une qualification / pré-production (non régression) au préalable dans l'environnement de qualification / pré-production. Elle doit faire l'objet d'une documentation ou d'une mise à jour de la documentation existante de la part des Exploitants (Système ou application en fonction de la nature du correctif).

Les procédures exécutées automatiquement sur les postes clients ne doivent pas utiliser de comptes ayant des privilèges permettant l'écriture sur des données distribuées à d'autres postes (notamment les packages installés).

Commentaires

Outre la non régression, la phase de qualification doit également permettre de valider la compatibilité des correctifs avec les différents mécanismes de sécurité (antivirus, mise à jour des packages...) et d'exploitation (supervision, administration, sauvegarde).

Comme pour toute opération de changement, les procédures d'installation des correctifs doivent garantir la possibilité de revenir à la configuration initiale en cas de dysfonctionnement.

SEE-22. Télédistribution

Les fichiers déposés sur les serveurs de mise à jour doivent être préalablement scannés par l'antivirus avant copie sur le serveur d'installation.

3.2.5. Reporting / tableaux de bord

SEE-23. Reporting

Les Exploitants adressent un reporting mensuel à la Maîtrise d'Ouvrage Sécurité, qui procède à la consolidation des indicateurs reçus pour construire des tableaux de bord Sécurité qui sont ensuite fournis au Comité de Direction de la DSI.

Commentaires

Ce reporting mentionne notamment :

- Un état des lieux relatif au déroulement des sauvegardes et des tests de restauration associés,
- Un état des habilitations accordées (notamment la liste des couples identifiants/authentifiants inutilisés, les droits d'accès associés aux partages réseaux...),
- Les incidents de sécurité constatés (défaut de mise à jour de la base de signature virale, indisponibilité complète ou partielle de l'équipement ou d'une application hébergée...) et les mesures mises en œuvre ou prévues,
- Les évolutions de capacités (mémoire, disque...), les périodes de surcharge et la raison de la surcharge (goulot d'étranglement réseau, mémoire insuffisante...),
- La liste et les résultats des principales actions de contrôle opérées sur les équipements.

SEE-24. Reporting pour un SIE

Dans le cadre d'un SIE, des indicateurs doivent être réalisés sur une période de 2 ans en regard des sujets suivants :

- Sur le maintien en conditions de sécurité des ressources,
- Sur les droits d'accès des utilisateurs et à l'authentification des accès aux ressources,
- Sur l'administration des ressources.

Ces indicateurs doivent être fournis au RSSI, en précisant les raisons d'une évolution significative le cas échéant.

Une communication sur ces indicateurs sera réalisée vers l'ANSSI par le RSSI.

Commentaires

Ces indicateurs sont les suivants :

- Maintien en conditions de sécurité des ressources :
 - ▶ Le pourcentage de postes utilisateurs dont les ressources systèmes ne sont pas installées dans une version supportée par le fournisseur ou le fabricant ;
 - ▶ Le pourcentage de serveurs dont les ressources systèmes ne sont pas installées dans une version supportée par le fournisseur ou le fabricant.
- Droits d'accès des utilisateurs et à l'authentification des accès aux ressources :
 - ▶ Le pourcentage d'utilisateurs accédant au SIE au moyen de comptes privilégiés ;
 - ▶ Le pourcentage de ressources dont les éléments secrets d'authentification ne peuvent pas être modifiés par l'opérateur.

■ Administration des ressources :

- ▶ Le pourcentage de ressources administrées dont l'administration est effectuée à partir d'un compte non spécifique d'administration;
- ▶ Le pourcentage de ressources administrées dont l'administration ne peut pas être effectuée au travers d'une liaison réseau physique ou d'une interface d'administration physique.

SEE-25. Evaluation des indicateurs d'un SIE

Dans le cadre d'un **SIE**, une procédure opérationnelle doit être tenue, décrivant les méthodes d'évaluation des indicateurs et, le cas échéant, la marge d'incertitude de son évaluation.

SEE-26. Journalisation des opérations d'exploitation

Toutes les modifications portant sur le paramétrage des événements à journaliser doivent être tracées. En outre, les journaux d'événements doivent être sauvegardés avant d'être effacés des systèmes.

Recommandation

Sauf avis contraire de la CNIL, il est recommandé de conserver les journaux d'événements pour une durée minimale d'un an.

4. ANNEXE

4.1. GLOSSAIRE

	Un changement peut être apporté pour réagir à un problème. Il peut également être imposé par des exigences externes (ex. : changements de la loi), être appliqué de façon proactive dans le but d'améliorer l'efficacité et l'efficacité ou de tenir compte de nouvelles contraintes métiers, ou bien découler de programmes, de projets ou d'initiatives visant à améliorer un service. La gestion des changements peut notamment :
Changement	■ assurer l'utilisation de procédures, de méthodes et de processus uniformes pour tous les changements, ■ faciliter le traitement rapide et efficace de tous les changements, ■ maintenir un équilibre entre la nécessité des changements et leurs conséquences néfastes potentielles.
Exploitation	Ensemble des tâches qui permettent d'assurer le bon fonctionnement au quotidien des Systèmes d'Information dans un souci de productivité, de respect de la sécurité et de la qualité de service aux utilisateurs.
Maintenance	Ensemble des tâches ayant pour objectif l'entretien des Systèmes d'Information et son adaptation aux modifications de son environnement (installation de correctifs...).
Média	Ce terme désigne les supports physiques de stockage de l'information (disque dur, bande magnétique, support optique,...).
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.
SIE	Un SIE (Système d'information essentielle) est un système d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.
Support	Opération permettant d'assurer une assistance technique. Elle s'adresse aux utilisateurs des Systèmes d'Information.
Télédistribution	Méthode de déploiement à distance d'une application (ou de ses mises à jours) sur plusieurs machines, à partir d'un poste maître.
Tiers	Le terme « Tiers » désigne l'ensemble des stagiaires, des prestataires, des fournisseurs, des partenaires et des travailleurs intérimaires employés à titre individuel par France Travail et amenés à travailler, de manière permanente ou occasionnelle, au profit des Systèmes d'Information et, de ce fait, à avoir accès à

leurs informations ou à leurs ressources.

4.2. LISTE DES RÈGLES

SEE-01.	Responsabilité des équipes de support.....	7
SEE-02.	Contrôle des opérations de support.....	7
SEE-03.	Responsabilité des Administrateurs et des Exploitants	9
SEE-04.	Administration et exploitation des composants des SI	10
SEE-05.	Administration et exploitation des composants d'un SIE	10
SEE-06.	Contractualisation des exigences pour les tiers	11
SEE-07.	Opérations d'infogérance externe ou de sous-traitance	11
SEE-08.	Gestion de parc	11
SEE-09.	Traçage des mouvements de matériels	12
SEE-10.	Modification de configuration d'un équipement	12
SEE-11.	Procédures de gestion des médias	13
SEE-12.	Protection et stockage des médias.....	13
SEE-13.	Externalisation du stockage des médias	13
SEE-14.	Gestion des sorties des médias	14
SEE-15.	Effacement des médias avant réutilisation	14
SEE-16.	Vérification des médias d'archivage	14
SEE-17.	Sécurité des locaux	15
SEE-18.	Protection des zones	16
SEE-19.	Protection des équipements d'administration des accès physiques	16
SEE-20.	Changement	17
SEE-21.	Installation des correctifs	17
SEE-22.	Télédistribution	17
SEE-23.	Reporting	18
SEE-24.	Reporting pour un SIE	18
SEE-25.	Evaluation des indicateurs d'un SIE	19
SEE-26.	Journalisation des opérations d'exploitation	19

(Fin de document)