POLITIQUE DE CONTRÔLE D'ACCÈS LOGIQUE ET PHYSIQUE

InfoTec86
Integrated Cloud & Telecom Solutions

Novembre 2025

InfoTEC86

Référence : PSSI-POL-06-001

Classification : INTERNE - INFOTEC86

Ce document définit les règles de sécurité pour l'accès aux systèmes d'information d'InfoTec86 (SaaS, IaaS, Bureaux). Il couvre le cycle de vie des identités, la gestion des mots de passe et la sécurisation physique des locaux.

www.InfoTEC86.com

Politique de Contrôle d'Accès Logique et Physique PSSI

Table des matières

Tableau de Suivi des Versions

Version	Date	Auteur	Vérificateur	Approbateur	Description des changements
1.0	12/11/2025	N. FRERE (RSSI) 16	J. Martin (CTO) 17	C. Leroy (DG) 18	Création initiale de la politique.

1. Objet

La présente politique définit les principes et les règles de gestion des accès logiques et physiques au Système d'Information (SI) et aux actifs d'InfoTec86.

Elle vise à protéger la confidentialité, l'intégrité et la disponibilité des informations et des services, notamment la plateforme Iris2.0, les infrastructures IaaS et les API partenaires, en s'assurant que l'accès est accordé sur la base des principes stricts du **besoin d'en connaître** et du **moindre privilège**.

Cette politique s'appuie sur les recommandations de la norme ISO 27002:2022, notamment les contrôles relatifs à la gestion des accès.

2. Domaine d'Application

Cette politique s'applique à:

- L'ensemble du personnel d'InfoTec86.
- Tous les tiers, prestataires, et partenaires ayant accès au SI d'InfoTec86.
- L'ensemble des actifs matériels et immatériels, y compris :
    - Les locaux d'InfoTec86 et les infrastructures hébergées dans les datacenters tiers.

- Les serveurs, équipements réseau et postes de travail.
- La plateforme Iris2.0, les bases de données clients et les API.
- L'ensemble des données, quel que soit leur niveau de classification.

3. Rôles et Responsabilités

- **Le RSSI** (Propriétaire):
  - Définit et maintient cette politique.
  - Supervise la gestion des comptes à privilèges et la revue des droits.
  - Approuve les demandes d'accès exceptionnels ou aux actifs classifiés "Confidentiel".
- **La DSI et le CTO**:
  - Implémentent et maintiennent les mesures techniques de contrôle d'accès (logiques et physiques).
  - Gèrent l'infrastructure des datacenters et l'accès sécurisé aux API.
  - Exécutent les révocations d'accès sur demande.
- **Les Ressources Humaines** (RH):
  - Sont responsables de la fiabilité du processus d'arrivée (Joiner), de mobilité (Mover) et de départ (Leaver).
  - Notifient formellement et sans délai le RSSI et la DSI de tout mouvement de personnel..
- **Les Managers** (Pilotes de processus) :
  - Définissent le "besoin d'en connaître" de leurs collaborateurs.
  - Valident formellement les demandes d'accès de leurs équipes.
  - Participent activement aux revues périodiques des droits d'accès.
- **L'Ensemble du personnel**:

- Est tenu de respecter cette politique.
- Doit protéger ses informations d'authentification (mots de passe, badges) et ne jamais les partager.

Les responsabilités concernant l'application de la présente politique sont définies selon le **modèle RACI** ci-dessous :

- **R** (Réalise) : Celui qui exécute la tâche.
- **A** (Approbateur) : Le responsable unique qui rend des comptes et valide le résultat.
- **C** (Consulté) : Celui qui apporte une expertise ou un avis avant la décision/action.
- **I** (Informé) : Celui qui est tenu au courant après l'action.

Activité / Processus	RSSI	DSI / CTO	RH	Managers	Personnel
Définition et maintien de la Politique d'Accès	A / R	C	I	I	I
Signalement des Mouvements (JML : Arrivée, Départ, Mobilité)	I	I	A / R	I	-
Définition du "Besoin d'en connaître"	A	C	-	R	-
Validation des demandes d'accès standards	I	-	-	A	-
Validation des accès "Confidentiel" ou Exceptionnels	A	I	-	R	-
Implémentation technique (Création/Révocation, Infra, API)	C	R	-	-	-
Supervision des comptes à privilèges	A	R	-	-	-
Revue périodique des droits	A	C	-	R	-

Activité / Processus	RSSI	DSI / CTO	RH	Managers	Personnel
Protection des authentifiants (Mots de passe, badges)	I	I	-	R	R

4. Principes Fondamentaux du Contrôle d'Accès

Toute gestion d'accès au sein d'InfoTec86 doit respecter les principes suivants :

4.1. Principe du Moindre Privilège

Les utilisateurs ne doivent disposer que des droits d'accès minimaux nécessaires à l'accomplissement de leurs missions. Tout droit supplémentaire doit être formellement justifié et approuvé.

(Réf. ISO 27002:2022 - Contrôle 5.18, 8.2)

4.2. Séparation des Tâches (SoD)

Les droits d'accès doivent être attribués de manière à éviter qu'une seule personne ne puisse exécuter une transaction critique de bout en bout (ex: développer, tester et mettre en production). Les comptes d'administration sont strictement séparés des comptes utilisateurs standards.

(Réf. ISO 27002:2022 - Contrôle 5.3)

4.3. Identification et Authentification Uniques

Chaque utilisateur (humain ou service) doit être identifié de manière unique. Les comptes génériques ou partagés sont interdits, sauf dérogation formelle du RSSI pour des besoins opérationnels spécifiques et tracés.

(Réf. ISO 27002:2022 - Contrôle 5.16, 5.17)

4.4. Modèle de Contrôle d'Accès (RBAC)

L'attribution des droits d'accès repose sur le modèle de **Contrôle d'Accès Basé sur les Rôles (RBAC)**.

- Les droits d'accès sont liés à la fonction (le rôle) exercée par l'utilisateur et non à son identité propre.
- Des profils métiers types sont définis et maintenus par les responsables de service.
- Toute demande d'accès doit se référer à l'un de ces profils prédéfinis. Les droits spécifiques "hors profil" (DAC) doivent rester l'exception.

Document associé : La définition des rôles est consignée dans la **Matrice des Rôles et Profils [PSSI-STD-06-004]**

(Réf. ISO 27002:2022 - Contrôle 5.15, 5.18)

4.5. Approche Zero Trust et Accès Conditionnel

En complément du modèle RBAC, InfoTec86 applique une politique d'**Accès Conditionnel** (Dynamic Access Control). L'autorisation d'accès est évaluée en temps réel en fonction du niveau de risque de la connexion.

- Les décisions d'accès prennent en compte le contexte : l'identité de l'utilisateur, l'état de sécurité du terminal (conformité), la localisation géographique et le comportement habituel.
- Si le risque détecté est élevé des mesures de remédiation automatiques sont appliquées (ex: exigence de MFA, blocage de l'accès).

Document associé : Les règles de contexte sont définies dans le **Standard de Politique d'Accès Conditionnel [PSSI-STD-06-005]**.

(Réf. ISO 27002:2022 - Contrôle 5.15, 8.5)

5. Cycle de Vie des Accès (Processus JML)

Ce processus est crucial pour limiter les risques liés aux comptes inactifs.

- **Document associé :** Voir la **Procédure de Gestion des Entrées/Sorties [PSSI-PRO-04-001]**.

5.1. Arrivée (Joiner)

Aucun accès n'est créé sans une demande formelle des RH. Les droits par défaut sont définis selon le principe du moindre privilège. L'utilisateur doit accuser réception de la PSSI.

(Réf. ISO 27002:2022 - Contrôle 5.16)

5.2. Mobilité (Mover)

Tout changement de poste ou de fonction doit déclencher une revue formelle des droits par le nouveau manager. Les anciens droits non pertinents doivent être révoqués avant l'octroi des nouveaux.

5.3. Départ (Leaver)

Dès la notification de départ par les RH, tous les accès (logiques et physiques, y compris VPN et badges) de l'employé doivent être désactivés au plus tard à la fin de son dernier jour de présence.

(Réf. ISO 27002:2022 - Contrôle 5.18)

5.4. Revue des Droits d'Accès

Une revue périodique des droits d'accès est obligatoire :

- Trimestrielle pour l'ensemble des comptes utilisateurs.
- Mensuelle pour tous les comptes à privilèges (Administrateurs Iris2.0, DSI, CTO, RSSI).

  Cette revue est pilotée par le RSSI et validée par les managers.

- **Document associé :** Voir la **Procédure de Revue des Habilitations [PSSI-PRO-06-002]**.

  (Réf. ISO 27002:2022 - Contrôle 5.18)

6. Contrôle d'Accès Logique

6.1. Authentification des Utilisateurs

- **Mots de passe :** Les mots de passe doivent respecter une complexité minimale (12 caractères, 3 types de caractères). Ils doivent être changés immédiatement en cas de suspicion de compromission. L'utilisation d'un gestionnaire de mots de passe (coffre-fort) approuvé par la DSI est obligatoire pour stocker les secrets.Le compte utilisateur est temporairement verrouillé après un nombre défini de tentatives de connexion infructueuses consécutives.
- **Authentification Multi-Facteurs (MFA) :** Le MFA est **obligatoire** pour :
  - Tout accès distant (VPN, services cloud externes).
  - L'accès aux interfaces d'administration (Iris2.0, serveurs IaaS, équipements réseau).
  - L'accès aux comptes à privilèges.
- **Document associé :** Voir le **Standard d'Authentification [PSSI-STD-06-001]**.

  (Réf. ISO 27002:2022 - Contrôle 5.17, 8.5)

6.2. Gestion des Accès à Privilèges (PAM)

Les comptes à privilèges (Admin, root, etc.) représentent un risque critique.

- Les comptes administrateurs doivent être nominatifs et distincts des comptes utilisateurs standards.
- L'utilisation de ces comptes est réservée exclusivement aux tâches d'administration (pas de navigation web ou de messagerie).
- Toutes les actions effectuées avec des comptes à privilèges doivent être journalisées et supervisées.
- Une procédure d'accès d'urgence est définie pour permettre l'accès aux systèmes critiques en cas de panne des mécanismes d'authentification nominaux. L'usage de ce compte générique de secours déclenche une alerte immédiate au RSSI.

- **Document associé :** Voir le **Standard Gestion des administrateurs [PSSI-STD-06-002]**.

  (Réf. ISO 27002:2022 - Contrôle 8.2)

6.3. Accès aux API et Tiers (PaaS)

Les accès fournis aux partenaires via les API doivent être sécurisés pour prévenir les fuites.

- Chaque partenaire doit disposer d'une clé d'API ou d'un compte de service unique.
- Les droits de ces accès doivent être limités aux seules fonctions nécessaires (moindre privilège).
- Les flux API doivent être chiffrés et leur usage doit être monitoré pour détecter toute activité anormale.

- **Document associé :** Voir le **Standard de Sécurité des Accès API [PSSI-STD-06-003]** .

  (Réf. ISO 27002:2022 - Contrôle 5.20, 5.21, 8.3)

6.4 - Ségrégation des Réseaux

Le réseau d'administration (management plane) des infrastructures Cloud (IaaS) est strictement isolé du réseau bureautique et du réseau public. L'accès à ce réseau d'administration se fait uniquement via des passerelles sécurisées (bastions/VPN d'administration) et nécessite une authentification forte.

- **Document associé :** Voir le **Standard de Sécurité Réseau [PSSI-STD-09-001]** .

  (Réf. ISO 27002:2022 - Contrôle 8.20, 8.22, 8.31)

6.5 - Accès Distant et Mobilité :

- L'accès aux ressources internes depuis l'extérieur des locaux d'InfoTec86 s'effectue exclusivement via le VPN d'entreprise sécurisé.

- Les équipements portables (PC, smartphones) contenant des données professionnelles doivent avoir leur disque dur intégralement chiffré (Full Disk Encryption) pour protéger les données en cas de vol ou de perte.
- **Document associé :** Voir le **Standard de Sécurité Réseau [PSSI-STD-09-001]** et le **Standard de Cryptographie [PSSI-STD-07-001]** .

(Réf. ISO 27002:2022 - 6.7, 8.1, 8.24)

6.6 - Journalisation et imputabilité :

- Les événements liés à la sécurité (connexions réussies et échouées, accès aux données sensibles, actions d'administration, usage de privilèges) doivent être journalisés.
- Les journaux doivent être conservés pendant une durée conforme aux exigences légales et réglementaires et protégés contre toute altération (principe d'intégrité des traces).
- Toute détection d'accès non autorisé ou suspect doit être traitée conformément à la **Procédure de Gestion des Incidents de Sécurité [PSSI-PRO-13-001]**.
- **Document associé :** Voir le **Standard de Journalisation et Audit [PSSI-STD-08-001],** le **Tableau de Rétention des Données et Enregistrements [PSSI-STD-01-001]** et la **Procédure de Gestion des Incidents de Sécurité [PSSI-PRO-13-001].**

(Réf. ISO 27002:2022 - Contrôle 8.15, 8.16)

7. Contrôle d'Accès Physique

7.1. Accès aux Locaux (Bureaux InfoTec86)

- L'accès aux bureaux est contrôlé par un système de badges nominatifs.
- Les locaux sont découpés en zones de sécurité distinctes (Zone Accueil, Zone Bureaux, Zone Technique/Serveurs). L'accès aux zones techniques est restreint à une liste nominative de personnel autorisé.
- Tous les visiteurs doivent être enregistrés, accompagnés et porter un badge visible.

- Une politique de "bureau propre et écran verrouillé" doit être appliquée pour réduire le risque de vol d'information.

- **Document associé :** Voir la **Procédure de Gestion des Accès Physiques [PSSI-PRO-05-001]** .

(Réf. ISO 27002:2022 - Contrôle 7.2, 7.3, 7.7)

7.2. Accès aux Zones Sécurisées (Datacenters Tiers)

L'accès physique aux serveurs hébergés constitue un risque majeur.

- L'accès physique aux datacenters est strictement interdit à tout personnel non autorisé.
- Une liste nominative du personnel (DSI/CTO) autorisé à y accéder est maintenue par le RSSI.
- Toute intervention doit être planifiée, tracée, et approuvée par le RSSI et respecter les procédures de sécurité du datacenter hôte.

- **Document associé :** Voir la **Procédure de Gestion des Accès Physiques [PSSI-PRO-05-001]** .

(Réf. ISO 27002:2022 - Contrôle 7.1, 7.2, 7.4)

7.3. Protection du Matériel

Pour prévenir le vol :

- Les serveurs et baies (racks) dans les datacenters doivent être physiquement verrouillés.
- Les équipements réseaux (switchs, routeurs) situés dans les bureaux doivent être situés dans des armoires de brassage verrouillées pour empêcher les branchements sauvages.
- Les postes de travail portables doivent être chiffrés et ne jamais être laissés sans surveillance dans des lieux publics.
- Les supports de stockage (disques durs, clés USB) doivent être chiffrés s'ils contiennent des données sensibles.

- **Document associé :** Voir le **Standard de Sécurisation Physique des Équipements [PSSI-STD-05-001]**.

  (Réf. ISO 27002:2022 - Contrôle 7.8, 7.9, 7.10)

8. Documents de Référence

- **Documents Internes :**
  - PSSI-PRO-01-001: Procédure de Gestion Documentaire.
  - PSSI-POL-03-001: Politique de Classification d'InfoTec86.
  - PSSI-STD-01-001: Tableau de Rétention des Données.
  - PSSI-STD-06-004: Matrice des Rôles et Profils.
  - PSSI-STD-06-005: Standard de Politique d'Accès Conditionnel.
  - PSSI-PRO-04-001: Procédure de Gestion des Entrées/Sorties.
  - PSSI-PRO-06-002: Procédure de Revue des Habilitations.
  - PSSI-STD-06-001: Standard d'Authentification.
  - PSSI-STD-06-002: Standard de Sécurité des Accès API.
  - PSSI-STD-09-001: Standard de Sécurité Réseau.
  - PSSI-STD-07-001: Standard de Cryptographie.
  - PSSI-STD-08-001: Standard de Journalisation et Audit.
  - PSSI-PRO-13-001: Procédure de Gestion des Incidents de Sécurité.
  - PSSI-PRO-05-001: Procédure de Gestion des Accès Physiques.
- **Normes et Réglementations :**
  - ISO/IEC 27001:2022.
  - Règlement Général sur la Protection des Données (RGPD).