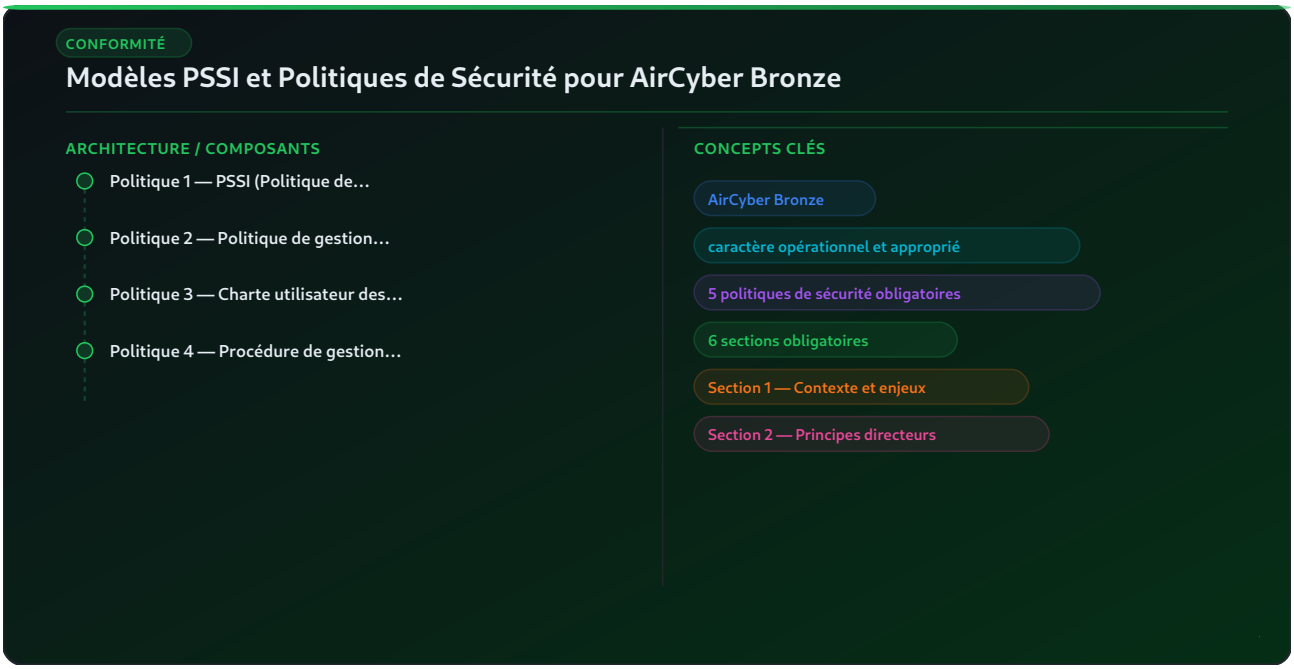
Modèles PSSI et Politiques de Sécurité pour AirCyber Bronze

AirCyber Bronze : PSSI, charte SI, gestion incidents, PCA. Structure et contenu minimal pour chaque politique. Points clés vérifiés par l'assesseur.

La documentation de sécurité constitue l'un des volets les plus chronophages — et les plus souvent sous-estimés — du parcours de labellisation **AirCyber Bronze**. L'assesseur accrédité BoostAerospace vérifie non seulement l'existence de chaque politique de sécurité, mais aussi leur **caractère opérationnel et approprié** à la taille et à l'activité de l'entreprise. Une politique copiée-collée depuis internet sans adaptation sera immédiatement identifiée comme non-conforme. Les **5 politiques de sécurité obligatoires** pour Bronze forment un ensemble cohérent qui couvre la gouvernance, la gestion des accès, le comportement des utilisateurs, la réponse aux incidents et la continuité d'activité. Ce guide détaille pour chacune la structure recommandée, le contenu minimal attendu par l'assesseur, et les pièges à éviter lors de la rédaction. Vous y trouverez aussi des conseils pratiques pour adapter rapidement un modèle existant à votre contexte spécifique, que vous soyez un équipementier de 20 salariés ou un intégrateur de 200 personnes. La qualité de cette documentation conditionne directement le bon déroulement de l'audit et la rapidité d'obtention du label.



Politique 1 — PSSI (Politique de Sécurité des Systèmes d'Information)

La *PSSI* est le document chapeau qui définit les ambitions, les principes et le cadre organisationnel de la sécurité dans votre entreprise. Pour AirCyber Bronze, elle doit couvrir **6 sections obligatoires** :

Section 1 — Contexte et enjeux : description de l'activité, périmètre du SI concerné, enjeux métier liés à la sécurité (données clients, propriété intellectuelle, continuité de production). Longueur recommandée : 1 à 2 pages.

Section 2 — Principes directeurs : les 5 à 8 principes fondamentaux de sécurité retenus par la direction (confidentialité, intégrité, disponibilité, conformité réglementaire). Ces principes doivent être **signés par le Directeur Général** — c'est un point de contrôle clé.

Section 3 — Organisation et responsabilités : organigramme de la sécurité (RSSI, responsable technique, correspondants métier), rôles et responsabilités définis, délégations formalisées.

Section 4 — Classification des informations : niveaux de sensibilité (Public / Interne / Confidentiel / Très Confidentiel), règles de traitement par niveau, exemples concrets adaptés à l'activité aéronautique (données CAO, plans de fabrication, données ITAR).

Section 5 — Cadre de conformité : référentiels applicables (Guide d'hygiène ANSSI, AirCyber, RGPD, NIS 2), articulation avec les exigences contractuelles clients.

Section 6 — Révision et mise à jour : fréquence de révision (annuelle minimum), conditions de révision exceptionnelle (incident majeur, changement SI significatif), processus d'approbation et de diffusion.

Point de contrôle assesseur : La PSSI doit porter une date de dernière révision de moins de 12 mois, une signature de la direction, et être diffusée à l'ensemble du personnel (preuve de diffusion exigée).

Politique 2 — Politique de gestion des mots de passe

La politique de **mots de passe** est l'une des plus vérifiées techniquement par l'assesseur, car il confronte le document avec la configuration réelle des systèmes (Active Directory, applications métier). Le contenu minimal requis :

> ⚡ **Retour terrain**
>
> Dans mes missions de conformité, j'observe que les entreprises sous-estiment systématiquement le délai de mise en œuvre des mesures techniques. Les mesures organisationnelles (politiques, procédures) s'écrivent en semaines ; les mesures techniques (segmentation réseau, chiffrement, MFA) se déploient en mois. Pour un plan de mise en conformité réaliste, je multiplie toujours les estimations initiales des équipes IT par 2,5 — et je n'ai jamais eu à réduire ce coefficient.

Complexité minimale : 12 caractères minimum (16 recommandés), majuscules/minuscules/chiffres/caractères spéciaux

Durée de validité : 90 jours pour les comptes standard, 60 jours pour les comptes administrateurs

Historique : interdiction de réutiliser les 10 derniers mots de passe

Authentification multi-facteurs (MFA) : obligatoire pour les accès distants, comptes privilégiés, messagerie

Gestionnaire de mots de passe : usage recommandé ou imposé pour les mots de passe complexes

Comptes de service : mots de passe distincts, rotation semestrielle, inventaire tenu à jour

Point de contrôle assesseur : L'assesseur demandera une démonstration de la configuration AD (longueur minimale, complexité, historique) et vérifiera que le MFA est effectivement activé sur les accès VPN et messagerie — pas seulement décrit dans la politique.

Politique 3 — Charte utilisateur des systèmes d'information

La *charte utilisateur SI* régit le comportement acceptable des employés sur le système d'information. Pour AirCyber Bronze, elle doit aborder :

Usages autorisés et interdits des équipements informatiques (personnel vs. professionnel)

Règles d'utilisation d'internet, messagerie et réseaux sociaux depuis les équipements de l'entreprise

Interdiction d'installation de logiciels non autorisés

Signalement des incidents et comportements suspects

Règles sur le travail nomade et le BYOD (Bring Your Own Device)

Conséquences disciplinaires en cas de violation

Point de contrôle assesseur : La charte doit être **signée par chaque employé** (attestation de prise de connaissance) et mise à jour lors de chaque modification majeure des conditions d'utilisation. Conservez les preuves de signature (numérique ou papier).

Politique 4 — Procédure de gestion des incidents de sécurité

Cette procédure décrit le **processus de bout en bout** depuis la détection d'un incident jusqu'à la clôture et le retour d'expérience. Structure recommandée pour AirCyber Bronze :

Phase 1 — Détection et qualification : canaux de remontée (email dédié, numéro d'astreinte), critères de qualification (incident mineur / majeur / critique), premiers réflexes (isolation d'un poste compromis, préservation des preuves).

Phase 2 — Réponse et confinement : responsable de la gestion de crise, actions techniques immédiates (blocage d'accès, sauvegarde forensique), communication interne (qui prévenir, comment).

Phase 3 — Notification : obligation de notification au **CERT Aviation** pour les incidents significatifs, notification à l'ANSSI si entité NIS 2 assujettie, information des clients si données compromises (RGPD 72h).

Phase 4 — Retour d'expérience : rapport post-incident obligatoire, identification des causes racines, plan d'action corrective, partage des enseignements en interne.

Point de contrôle assesseur : L'assesseur demande le **registre des incidents** des 12 derniers mois. Même en l'absence d'incident majeur, les incidents mineurs (tentatives de phishing, mises à jour bloquées) doivent être tracés. Un registre vide est considéré comme suspect.

Politique 5 — Plan de Continuité d'Activité (PCA/PRA simplifié)

Le *PCA/PRA simplifié* pour AirCyber Bronze n'exige pas le niveau de sophistication d'un PCA ISO 22301, mais doit couvrir les scénarios critiques pour l'activité aéronautique :

Inventaire des actifs critiques : systèmes et données dont l'indisponibilité bloque la production ou les livraisons

RTO/RPO définis : durée maximale d'indisponibilité acceptable et perte de données maximale tolérable par système

Procédures de reprise : étapes documentées pour restaurer chaque système critique depuis les sauvegardes

Tests annuels : au moins un test de restauration par an avec résultats documentés

Contacts de crise : liste des prestataires clés (hébergeur, MSP, éditeurs), astreintes internes
Point de contrôle assesseur : Les **preuves de tests** (rapport de restauration, compte-rendu d'exercice) sont exigées. Un PCA jamais testé est une non-conformité. Planifiez un test de restauration dans les 3 mois précédant votre audit.

Conseils pour adapter rapidement un modèle existant

Si vous partez d'un modèle générique (ANSSI, CNIL, template secteur), voici les adaptations prioritaires :

Remplacez toutes les références génériques par le **nom réel de votre entreprise et vos systèmes**

Adaptez les exemples de données sensibles à votre activité (plans CAO, données ITAR, données clients aéro)

Intégrez les **outils réellement utilisés** (AD, messagerie, ERP, PLM) avec leurs configurations actuelles

Ajoutez les contacts réels (RSSI, DSI, DG) avec coordonnées vérifiées

Faites valider le contenu par **les utilisateurs concernés** avant signature de la direction
Pour aller plus loin, consultez notre service d'accompagnement AirCyber et notre Centre de Ressources AirCyber qui propose des modèles pré-adaptés à la filière aéronautique.

À RETENIR

Points clés à retenir

✓ **5 politiques obligatoires** : PSSI, mots de passe, charte SI, incidents, PCA

✓ **PSSI signée DG** : point de contrôle non négociable, datée de moins de 12 mois

✓ **Preuves d'application** : signatures des chartes, registre incidents, rapport test PCA

✓ **MFA vérifié techniquement** : la politique doit correspondre à la configuration réelle

✓ **Modèles à adapter** : ne jamais soumettre un template générique sans personnalisation profonde

FAQ : Politiques de sécurité AirCyber Bronze

Les 5 politiques doivent-elles être dans des documents séparés ou peuvent-elles être regroupées ?

Les deux formats sont acceptés par les assesseurs. Un document unique structuré en chapitres facilite la maintenance et la cohérence. Cependant, pour la charte utilisateur, un document séparé est souvent préférable car il doit être signé individuellement par chaque employé — un document intégré dans la PSSI complète serait difficile à faire signer de manière ciblée.

Faut-il traduire les politiques si l'entreprise a des employés non-francophones ?

Si votre personnel inclut des employés ne maîtrisant pas le français, la traduction de la charte utilisateur est nécessaire pour que la signature soit valide (consentement éclairé). Pour les autres politiques, la version française suffit dès lors que les responsables concernés (RSSI, DSI) maîtrisent le français.

À quelle fréquence les politiques doivent-elles être révisées pour maintenir la labellisation Bronze ?

Une révision annuelle est le minimum requis, même si aucune modification substantielle n'est apportée. La révision doit être formellement documentée (date, auteur, motif, validation direction) même si la conclusion est "aucun changement nécessaire". Des révisions intermédiaires sont attendues en cas d'incident majeur, de changement important du SI, ou d'évolution réglementaire significative.

Articles complémentaires

→ Guide complet : obtenir la labellisation AirCyber Bronze

→ Checklist des 44 mesures ANSSI AirCyber Bronze

→ Liste des documents à préparer pour l'audit AirCyber

→ Choisir son assesseur AirCyber accrédité

Besoin d'aide pour rédiger vos politiques AirCyber ?

Nos experts vous fournissent des modèles pré-adaptés à votre secteur et accompagnent la personnalisation pour maximiser vos chances lors de l'audit assesseur.

Demander les modèles documentaires →

Mise en œuvre pratique : étapes et livrables

La conformité réglementaire génère une documentation substantielle qui doit être maintenue à jour et accessible lors des audits. Une organisation structurée de ces livrables simplifie considérablement les exercices de conformité et réduit le temps consacré à leur préparation.

Livrables documentaires essentiels

Quel que soit le référentiel de conformité concerné, les livrables fondamentaux incluent : un registre des traitements (obligatoire RGPD, utile pour tout SMSI) maintenu par le DPO ou le

RSSI ; une politique de sécurité de l'information (PSI ou PSSI) approuvée par la direction et diffusée à tous les collaborateurs ; des procédures opérationnelles documentées pour les processus critiques (gestion des incidents, accès privilégiés, sauvegardes) ; un plan de continuité d'activité (PCA) testé annuellement ; et des rapports d'audit internes et de revue de direction formalisés. Ces documents constituent le «squelette» du SMSI et sont systématiquement vérifiés lors des audits de certification.

Gouvernance et responsabilités

La conformité réglementaire est un effort collectif qui ne peut pas reposer uniquement sur le RSSI ou le DPO. Une gouvernance efficace définit clairement les rôles : le COMEX assume la responsabilité globale de la conformité (risque financier et réputationnel) ; les DSI et RSSI mettent en œuvre les mesures techniques ; les métiers identifient les données et processus critiques à protéger ; et les DPO/compliance officers assurent la cohérence réglementaire. Les comités de sécurité trimestriels, impliquant toutes ces parties prenantes, garantissent l'alignement entre les exigences réglementaires et les capacités opérationnelles de l'organisation. Le suivi des actions de remédiation dans un outil de GRC (Governance, Risk & Compliance) formalise ce processus et facilite la production des preuves d'audit.

Sanction et contrôle : ce que les autorités vérifient

Comprendre les priorités de contrôle des autorités de régulation permet aux organisations de concentrer leurs efforts sur les domaines qui font l'objet d'une surveillance accrue. Les autorités de supervision (CNIL, ANSSI, ACP pour le secteur bancaire, HAS pour le secteur santé) publient régulièrement leurs priorités de contrôle.

Priorités de contrôle 2025-2026

Les domaines prioritaires identifiés par les autorités françaises pour 2025-2026 : la sécurité des données de santé (contrôles HDS en forte augmentation suite aux incidents hospitaliers) ; l'IA et

le traitement des données personnelles (CNIL a annoncé 300 mises en demeure liées à l'IA en 2025) ; les sous-traitants et tiers (vérification des DPA et des audits de sécurité des fournisseurs) ; et la notification des violations de données dans les délais légaux (72h RGPD, 24h NIS 2 pour les entités essentielles). Les organisations qui documentent proactivement leur conformité dans ces domaines réduisent significativement leur exposition aux sanctions et bénéficient généralement d'une procédure d'audit moins contraignante.

Programme de préparation aux audits

Un programme structuré de préparation aux audits réduit le stress et améliore les résultats. Douze mois avant un audit de certification : gap analysis interne pour identifier les non-conformités. Six mois avant : corrections des écarts majeurs et préparation de la documentation. Trois mois avant : audit blanc interne conduit par un consultant externe indépendant. Un mois avant : formation des équipes sur les procédures et livrables à présenter. Cette approche systématique, validée par des centaines d'organisations certifiées ISO 27001, transforme l'audit de certification d'une épreuve redoutée en une validation formelle d'un travail déjà accompli.

Bonnes pratiques et recommandations complémentaires

Au-delà des techniques et outils présentés dans cet article, plusieurs principes transverses guident les professionnels de la cybersécurité dans leur approche quotidienne. La défense en profondeur (*defense-in-depth*) reste le principe fondateur : aucune mesure de sécurité unique n'est suffisante, et la multiplication des couches de protection — même imparfaites individuellement — crée une résilience globale supérieure à la somme de ses parties.

Veille et mise à jour continue

La cybersécurité est un domaine où l'obsolescence est rapide. Une technique ou un outil efficace en 2024 peut être contourné en 2026. Les équipes sécurité maintiennent leur efficacité en s'appuyant sur des sources de veille fiables : bulletins CERT-FR et ANSSI, advisories des

éditeurs (Microsoft MSRC, Google Project Zero, Cisco Talos), recherches académiques (USENIX Security, IEEE S&P, CCS), et publications de la communauté (threat intel reports des grands éditeurs, articles de blog de chercheurs reconnus).

Documentation et partage de connaissances

La capitalisation des connaissances est un enjeu organisationnel critique dans les équipes de sécurité. Les runbooks d'investigation, les post-mortems d'incidents, les procédures de réponse documentées, et les bases de connaissance internes permettent de maintenir la cohérence des pratiques indépendamment des rotations d'équipe et de réduire le temps de résolution des incidents récurrents. L'utilisation d'un wiki sécurisé (Confluence, Notion avec contrôles d'accès stricts) pour centraliser ces connaissances est une pratique adoptée par la majorité des équipes SOC matures. La documentation proactive, rédigée juste après les incidents pendant que les détails sont frais, est systématiquement plus précise et utile que la documentation rédigée après coup.

Points d'attention avancés pour les auditeurs et RSSI

Au-delà de la conformité de surface, les auditeurs expérimentés et les RSSI cherchent à évaluer la robustesse réelle du dispositif de sécurité. Ce niveau d'analyse requiert de dépasser la vérification documentaire pour s'intéresser à l'efficacité opérationnelle des contrôles.

Pièges courants dans les audits de conformité

Plusieurs patterns d'échec reviennent régulièrement lors des audits de renouvellement. La conformité sur papier sans effectivité opérationnelle : des politiques formalisées mais non appliquées, des procédures documentées mais inconnues des équipes, des contrôles déclarés actifs mais non supervisés. La dérive post-certification : les organisations qui traitent la certification comme une fin en soi plutôt que comme un jalons d'un processus continu connaissent systématiquement une dégradation de leur posture sécurité entre deux audits. La

gestion insuffisante des tiers : plus de 60% des violations impliquent un fournisseur ou un prestataire, mais les contrats de sous-traitance et les audits tiers sont souvent les parents pauvres des programmes de conformité. Adresser ces trois points avant l'audit réduit significativement le risque de non-conformité majeure.

Métriques de maturité à présenter en audit

Les auditeurs modernes s'intéressent aux indicateurs de fonctionnement réel du SMSI plutôt qu'à la simple existence des documents. Préparer : statistiques de gestion des incidents sur 12 mois (nombre, délai de traitement, taux de récidive) démontrant une amélioration continue ; résultats des exercices de continuité avec les actions correctives entreprises ; données de sensibilisation (taux de participation aux formations, taux d'échec aux simulations de phishing) ; et résultats des audits internes avec suivi des actions de remédiation. Ces métriques transforment l'audit en démonstration de la maturité de l'organisation plutôt qu'en exercice de conformité documentaire, et constituent la meilleure défense contre les questions inattendues des auditeurs sur l'efficacité opérationnelle des contrôles.

Checklist de mise en œuvre et points de contrôle

La mise en pratique des recommandations de cet article nécessite une approche structurée. Cette checklist synthétise les points de contrôle essentiels pour évaluer l'état d'avancement de votre déploiement et identifier les actions prioritaires.

Phase de préparation et d'inventaire

Avant toute action technique, constituer un inventaire précis est indispensable. Les éléments à recenser : cartographie exhaustive des actifs concernés (systèmes, applications, flux de données) avec leur criticité métier associée ; identification des propriétaires techniques et fonctionnels pour chaque actif ; évaluation du niveau de maturité actuel à partir des référentiels reconnus (CIS Controls, ISO 27001, NIST CSF) ; et documentation des dépendances entre composants pour

anticiper les impacts des modifications. Un inventaire incomplet génère des angles morts qui deviennent des vecteurs d'attaque exploitables par des acteurs malveillants disposant d'informations accessibles publiquement (OSINT, Shodan, LinkedIn).

Phase de déploiement et validation

Le déploiement progressif réduit les risques d'interruption de service et facilite la détection des régressions. Adopter un modèle de déploiement par vagues (wave deployment) : d'abord les environnements de développement et de test pour valider les configurations, ensuite les systèmes non-critiques en production, enfin les systèmes critiques lors de fenêtres de maintenance planifiées. Chaque vague s'accompagne d'une validation fonctionnelle complète et d'une période d'observation des métriques de performance et de sécurité. Un plan de retour arrière documenté et testé est obligatoire avant toute opération sur un système critique. Les critères de succès doivent être définis avant le déploiement, non après — un taux de faux positifs inférieur à 5% pour les alertes de sécurité, une disponibilité maintenue au niveau SLA contractuel, et l'absence d'incidents de sécurité liés aux modifications.

Phase de supervision et d'amélioration continue

La mise en place d'indicateurs de suivi permet de mesurer l'efficacité des mesures déployées et de justifier leur maintien auprès de la direction. Tableau de bord mensuel recommandé : nombre d'alertes générées par catégorie (critique, majeur, mineur) avec tendance sur 6 mois ; taux de couverture des actifs critiques par les contrôles de sécurité ; délai moyen de remédiation des vulnérabilités par sévérité CVSS ; et résultats des tests de régression mensuels sur les règles de détection. Ce tableau de bord, présenté en comité de sécurité, constitue la base d'un dialogue constructif entre les équipes techniques et le management sur les priorités d'investissement en cybersécurité.