Plan d’Assurance Sécurité

V.25.04

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

eurécia

Introduction

Objectifs de la politique de sécurité

La politique de sécurité de l'information de EURECIA a pour objectif principal d'assurer la confidentialité, l'intégrité et la disponibilité des informations au sein de l'organisation. Cette politique vise à établir un cadre de gestion de la sécurité de l'information qui protège les actifs informationnels contre les menaces potentielles, qu'elles soient internes ou externes.

Les objectifs spécifiques de cette politique incluent :

- **Protection des données personnelles** : Garantir la conformité avec le Règlement Général sur la Protection des Données (RGPD) et d'autres réglementations applicables en matière de protection des données personnelles, en veillant à ce que les informations des clients, employés et partenaires soient traitées de manière sécurisée et confidentielle.
- **Évaluation et gestion des risques** : Mettre en place une méthodologie d'analyse des risques afin d'identifier, évaluer et atténuer les risques liés à la sécurité de l'information, en s'assurant que les mesures de sécurité mises en œuvre sont proportionnelles aux risques identifiés.
- **Sensibilisation et formation** : Promouvoir une culture de la sécurité au sein de l'organisation à travers des programmes de sensibilisation et de formation réguliers, afin de garantir que tous les employés comprennent leurs rôles et responsabilités en matière de sécurité de l'information.
- **Continuité des activités** : Assurer la mise en place de plans de continuité et de reprise d'activité pour garantir que l'organisation peut maintenir ses opérations critiques et récupérer rapidement en cas d'incident de sécurité ou de sinistre.
- **Amélioration continue** : Établir un processus de révision et d'amélioration continue de la politique de sécurité de l'information, en tenant compte des retours d'expérience, des audits et des évolutions réglementaires afin de garantir la pertinence et l'efficacité des mesures en place.

Portée et applicabilité

Cette politique s'applique à l'ensemble du personnel et à toutes les parties prenantes impliquées dans la gestion, le traitement ou l'accès aux informations. Elle est destinée à garantir que tous les acteurs comprennent leurs responsabilités en matière de sécurité et que des mesures appropriées sont mises en œuvre pour protéger les actifs informationnels de l'organisation.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

La portée et l'applicabilité de cette politique seront régulièrement révisées pour s'assurer qu'elles restent adaptées aux évolutions des besoins de l'organisation, des risques liés à la sécurité de l'information, et des exigences réglementaires.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Contexte Organisationnel

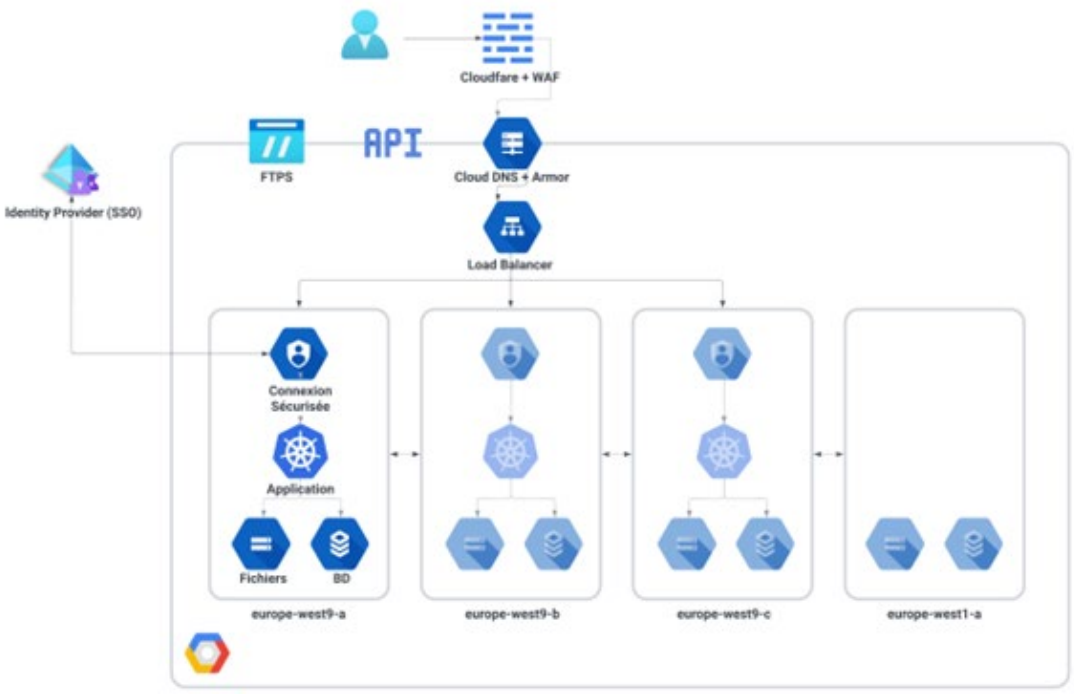
Présentation de l'organisation

EURECIA est une entreprise française fondée en 2006 basée à Castanet-Tolosan. EURECIA a développé une plateforme Internet de services aux entreprises diffusée en mode Software As A Service (SAAS) présentée sur son site officiel accessible à l'adresse www.eurecia.com. Eurécia est une solution tout-en-un pour répondre aux enjeux d'expérience, de performance et d'impact.

Eurécia est convaincue que l'épanouissement des collaborateurs est un facteur clé de la performance de l'entreprise. Afin d'accompagner les entreprises sur leurs enjeux humains, Eurécia leur propose une solution digitale complète, globale et modulable pour faciliter la gestion quotidienne des ressources humaines et optimiser les pratiques RH et managériales. L'automatisation des processus permet ainsi aux équipes RH de se concentrer sur des missions à forte valeur ajoutée, tout en améliorant l'expérience collaborateur.

Dans cette dynamique de construire un monde meilleur, Eurécia est également engagée dans une démarche de responsabilité sociétale des entreprises (RSE), laquelle a obtenu le label "Engagé RSE" niveau Confirmé de l'AFNOR.

Infrastructure technologique



3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Hébergement

Dans le cadre de sa stratégie de sécurité et de continuité de service, nous avons opté pour Google Cloud Platform (GCP) comme fournisseur d'hébergement pour des données. Ce choix repose sur plusieurs critères clés, garantissant à la fois la conformité aux exigences légales et la sécurité des données tout en optimisant les performances et la résilience de ses services :

- **Implantation géographique** : GCP respecte l'exigence de stockage des données exclusivement en France, conformément aux réglementations en vigueur et à la politique de souveraineté des données de l'entreprise.
- **Performance** : Google Cloud Platform offre des ressources de haute performance adaptées aux besoins évolutifs de l'entreprise, assurant une infrastructure flexible et scalable.
- **Sécurité** : GCP met en place des dispositifs robustes pour protéger les données. Ces mesures sont validées par des certifications reconnues telles que :
    - ISO 50001 (Systèmes de management de l'énergie),
    - European Code of Conduct for Cloud Providers,
    - Règlement Général sur la Protection des Données (RGPD),
    - ISO 27001 (Gestion de la sécurité de l'information).

Ces certifications assurent que les données sont protégées conformément aux standards internationaux de sécurité et aux exigences légales, renforçant ainsi la confiance dans l'infrastructure cloud de Google.

- **Responsabilité Sociétale des Entreprises (RSE)** : GCP s'engage activement en matière de développement durable, en visant la neutralité carbone et en investissant dans des technologies de cloud computing plus respectueuses de l'environnement.

Les services de GCP sont répartis sur trois datacenters localisés dans la région parisienne, garantissant ainsi la proximité géographique des données avec les utilisateurs finaux en France.

Dans un souci constant de sécurité et de disponibilité, les données sont régulièrement synchronisées en temps réel vers un datacenter secondaire situé en Belgique. Cette réplication géographique est conforme aux bonnes pratiques de sécurité, garantissant une continuité de service optimale en cas d'incident majeur dans la région parisienne.

Pour plus de détails sur les certifications et garanties offertes par GCP, vous pouvez consulter la liste complète disponible à l'adresse suivante :

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

https://cloud.google.com/security/compliance/offerings?hl=fr#/countries=EU_members®ions=EMEA.

Actifs informationnels

Chaque technologie utilisée par Eurécia a une valeur clé pour assurer une **protection totale des données** que nos clients nous confient :

- **Java/Kotlin (Spring, Hibernate)** : Ces langages et frameworks permettent de garantir une gestion sécurisée des données et des transactions, avec des mécanismes de contrôle d'accès, de validation des données et de prévention des vulnérabilités, assurant ainsi la confidentialité et l'intégrité des informations traitées.
- **PHP (Laravel, Eloquent)** : Ces technologies offrent une gestion structurée des bases de données avec des protections contre les injections SQL et un hachage sécurisé des mots de passe. Elles permettent de sécuriser les données sensibles lors de leur stockage et de leur traitement.
- **Typescript (Vue.js)** : Ces outils permettent de créer des interfaces utilisateurs sécurisées et réactives. Grâce à une gestion stricte des sessions et de la communication avec le backend, ils minimisent les risques d'exposition des données sensibles.
- **Serveurs Linux Debian** : Debian garantit un environnement stable et sécurisé, avec des mécanismes de protection avancés tels que des mises à jour régulières de sécurité, le contrôle des accès et la gestion des permissions pour protéger les données stockées et traitées.
- **Apache et Tomcat** : Ces serveurs assurent une gestion sécurisée des requêtes et des sessions, avec des configurations adaptées pour prévenir les attaques et garantir la sécurité des données en transit grâce à HTTPS.
- **MySQL et MongoDB** : Ces bases de données permettent de stocker les données sensibles de manière sécurisée, en offrant des fonctionnalités de chiffrement des données au repos et en transit, ainsi qu'une gestion fine des accès et des transactions sûres.
- **RabbitMQ** : Ce système de gestion des messages assure une communication sécurisée entre les composants, avec des mécanismes de contrôle d'accès et de chiffrement, garantissant que les messages contenant des informations sensibles restent protégés.

L'ensemble de ces technologies forme un écosystème cohérent qui assure la sécurité, la confidentialité et l'intégrité des données des clients à chaque étape de leur traitement et de leur stockage

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

eurécia

Parties prenantes

Finalités	Sous-traitants	Localisation des serveurs	Transferts	Garanties appropriées
Hébergement	Google Cloud Platform	France	Aucun transfert hors UE effectué	Aucune garantie appropriée requise
Hébergement des bases de données utilisateurs	Google Cloud Platform	France	Aucun transfert hors UE effectué	Aucune garantie appropriée requise
Dépôt et utilisation des cookies statistiques	Amplitude	Amplitude (Union Européenne)	Amplitude (aucun transfert hors UE effectué)	Amplitude (aucune garantie appropriée requise)
	Datadog	Datadog (Allemagne)	Datadog (aucun transfert hors UE effectué)	Datadog (aucune garantie appropriée requise)
	Hotjar	Hotjar (Irlande)	Hotjar (aucun transfert hors UE effectué)	Hotjar (aucune garantie appropriée requise)
	Google analytics 4	Google analytics 4 (Etats-Unis)	Google analytics 4 (transferts vers les Etats-Unis effectués)	Google analytics 4 (clauses contractuelles standards)
	Appcues	Appcues (Etats-Unis)	Appcues (transferts vers les Etats-Unis effectués)	Appcues (décision de certification accord UE-US)
Notifications techniques à destination des utilisateurs de la plateforme Eurécia	Mailgun	Etats-unis	Transferts vers les Etats-Unis effectués	Clauses contractuelles standards

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Utilisation de serveurs CDN pour améliorer la performance de la plateforme Eurécia	Cloudflare	France	Aucun transfert hors UE effectué	Aucune garantie appropriée requise
Coffre-fort numérique (Uniquement pour les clients bénéficiant du coffre-fort)	Edoc	France	Aucun transfert hors UE effectué	Aucune garantie appropriée requise

Mesures de Sécurité

Sécurité des accès

Authentification et gestion des identités

Il existe 2 méthodes d'authentification possibles, celle par identifiant et mot de passe avec une gestion des règles de changement de mot de passe, ou celle par SSO qui permet au client une plus grande maîtrise et autonomie ainsi que la possibilité d'intégrer un MFA (ou 2FA) via votre SSO.

Gestion des mots de passe

Les mots de passe des utilisateurs doivent impérativement respecter les critères suivants :

1. **Longueur minimale** : Le mot de passe doit comporter **au moins 12 caractères**. Cette exigence vise à renforcer la robustesse du mot de passe et à limiter les risques d'attaque par force brute.
2. **Complexité** : Le mot de passe doit contenir obligatoirement :
    a. Au moins **1 lettre majuscule**,
    b. Au moins **1 lettre minuscule**,
    c. Au moins **1 chiffre**,
    d. Et au moins **1 caractère spécial** parmi les suivants : **!@#$%^&*()-+**.

Ces critères permettent de garantir une complexité suffisante pour protéger les comptes utilisateurs contre les tentatives d'intrusion.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

3. **Rotation des mots de passe** : Le nouveau mot de passe doit impérativement être **différent des 3 derniers mots de passe** utilisés. Cette mesure permet de limiter les risques liés à la réutilisation de mots de passe et à leur éventuelle compromission.
4. **Limitation des tentatives d'authentification** : Pour protéger contre les attaques par **force brute** ou **tentatives multiples**, le nombre de tentatives d'authentification à la plateforme Eurécia est limité à **5 tentatives**. Après ces 5 tentatives infructueuses, le compte de l'utilisateur sera **bloqué pendant 15 minutes**, afin de prévenir les accès non autorisés.

Ces règles sont conçus pour répondre aux exigences de sécurité les plus élevées, en conformité avec les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) et de la CNIL (Commission Nationale de l'Informatique et des Libertés).

Single Sign-On

Le système de **Single Sign-On (SSO)** avec le protocole **SAML 2.0** offre un niveau de sécurité renforcé pour les utilisateurs d'Eurécia. En déléguant l'authentification à un **Identity Provider** (ex : LDAP) géré par la Direction des Systèmes d'Information (DSI) du client qui va centraliser la gestion des identifiants et des droits d'accès. Ainsi Eurécia n'accède qu'aux informations strictement nécessaires à l'authentification, minimisant ainsi les risques liés à la gestion des mots de passe.

Ce processus réduit l'exposition aux attaques par **phishing** et autres vulnérabilités liées aux mots de passe, tout en offrant un contrôle plus strict sur les accès. Le SSO améliore également la traçabilité des connexions et permet une gestion plus précise des permissions, garantissant que chaque utilisateur dispose uniquement des droits nécessaires à ses fonctions.

Ainsi, le SSO assure une **protection renforcée des données sensibles**, une gestion centralisée des accès et une réduction des risques de compromission des identifiants, tout en simplifiant l'expérience utilisateur.

Sécurité des données

Mesures prises pour protéger les données sensibles et garantir leur sécurité.

Chiffrement des données (au repos et en transit)

Eurécia applique des mécanismes de chiffrement robustes pour protéger les données sensibles tout au long de leur traitement et stockage.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

- **Mots de passe** : Un **algorithme irréversible** basé sur **SHA-256** est utilisé pour garantir la sécurité des mots de passe. Même en cas d'accès non autorisé aux données, les mots de passe ne peuvent pas être récupérés.
- **Données sensibles** : Pour les informations sensibles, telles que les données bancaires, un **algorithme réversible** est appliqué, permettant leur déchiffrement sécurisé uniquement pour les utilisateurs ou systèmes autorisés.
- **Données au repos et en transit** : **Google Cloud Platform (GCP)** chiffre toutes les données stockées sur disque avec l'algorithme **AES-256**, garantissant une protection maximale contre toute tentative d'accès non autorisé.

Ces mesures assurent une **protection complète des données**, qu'elles soient en transit ou stockées, et renforcent la confidentialité et l'intégrité des informations sensibles des utilisateurs.

Cloisonnement des données

Le cloisonnement des données est assuré par un TENANT_ID associé à chaque client, utilisé dans chaque requête et lié à chaque objet métier stocké en base de données. L'application Eurécia gère la sécurité sur l'ensemble des transactions effectuées au travers de cet ID qui est validé avec l'utilisateur en session.

Sauvegardes et récupération

Nous mettons en place une politique de **sauvegarde et de récupération des données** rigoureuse afin de garantir la continuité de service et la protection des informations sensibles de nos utilisateurs.

- **Sauvegardes régulières** : Nous effectuons **deux sauvegardes par jour**, assurant ainsi une copie actualisée de l'ensemble des données critiques. Ces sauvegardes sont automatisées et vérifiées pour garantir leur intégrité.
- **Duplication géographique** : Afin de renforcer la résilience de notre infrastructure, nous **duplication ces sauvegardes dans deux autres datacenters**, situés dans des régions géographiques distinctes. Cela permet de garantir la disponibilité des données en cas de défaillance dans l'un des sites, minimisant ainsi le risque de perte de données.
- **Objectifs de délai de reprise (RTO)** : En cas d'incident, nous nous engageons à rétablir les services dans un délai maximal de **4 heures**. Cet objectif nous permet de garantir une reprise rapide de l'activité, minimisant ainsi l'impact pour nos utilisateurs.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

- **Objectifs de point de reprise (RPO)** : Nous nous fixons un objectif de **5 heures** maximum pour le point de reprise, ce qui signifie que, en cas de défaillance, les données peuvent être restaurées à un état ne datant pas de plus de 5 heures.

Protection des données personnelles

Les données que vous nous confiez sont précieuses et toute l'équipe Eurécia est mobilisée pour assurer leur sécurité.

Toutes les données sauvegardées sur vos bases sont **absolument confidentielles.** Tous les collaborateurs sont soumis à une stricte confidentialité via une clause relative à la protection des données personnelles et sont formés et sensibilisés à la sécurité des données.

Par conséquent, Eurécia a nommé un DPO. Vous trouverez en annexe de ce document :

- L'attestation de désignation du DPO
- Label « RGPD Conforme » établit par notre DPO Externalisé : Dipeeo

Traçabilité

Tous les accès, qu'ils soient externes ou internes (support, paramétrage, etc.), sont **historisés** de manière détaillée. Cette **journalisation** permet de suivre les actions réalisées par chaque utilisateur, assurant une traçabilité complète des opérations effectuées.

Toutefois, pour des questions de confidentialité et de respect de la vie privée de nos utilisateurs, nous ne serons pas en mesure de répondre à toute demande de vérification de connexion (diffusion des adresses IP ou localisation géographique).

Nous accompagnons nos clients lorsqu'ils le demandent mais nous veillons au **strict respect de l'application du RGPD.** La **durée de rétention** des logs est fixée à **60 jours calendaires**, après quoi les données sont supprimées de manière automatisée et sécurisée, assurant la conformité avec nos engagements en matière de sécurité et de confidentialité.

Sécurité réseau

Pour garantir une **protection optimale contre les attaques externes** et assurer la sécurité de nos infrastructures, Eurécia met en place une **segmentation réseau** rigoureuse et des dispositifs de **sécurisation avancée**.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

- **Cloudflare et Cloud Armor (GCP)** : Nous utilisons **Cloudflare** pour la gestion du trafic entrant, offrant ainsi une protection contre les attaques par déni de service distribué (DDoS) et autres menaces. Associé à **Cloud Armor**, le service de **protection des applications** de Google Cloud Platform, nous bénéficions d'une défense renforcée contre les attaques ciblant nos applications et infrastructures.
- **WAF (Web Application Firewall) de Cloudflare** : Le **WAF de Cloudflare** permet de filtrer et bloquer le trafic malveillant avant qu'il n'atteigne nos systèmes. Ce pare-feu d'application web analyse les requêtes HTTP/HTTPS entrantes et les compare à des règles de sécurité prédéfinies pour détecter et contrer des attaques telles que l'injection SQL, le cross-site scripting (XSS) et autres vulnérabilités courantes.
- **Réseaux séparés pour les environnements** : Nos environnements de développement, de test et de production sont isolés sur des **réseaux séparés**, ce qui minimise les risques de propagation d'incidents de sécurité. Cette segmentation permet également d'assurer une gestion stricte des accès et de réduire la surface d'attaque potentielle.
- **Accès restreint en fonction des environnements** : Les accès aux différents environnements sont strictement **restreints** et **contrôlés**. Seul le personnel autorisé peut accéder aux environnements de production, et les droits d'accès sont accordés en fonction des rôles et des besoins spécifiques de chaque utilisateur. Cette gestion des accès renforce la sécurité et garantit que seules les personnes autorisées peuvent interagir avec des données sensibles ou des ressources critiques.

Sécurité physique

Locaux GCP

Les centres de données sont conçus avec la **sécurité au cœur de leur fonctionnement**. Ils utilisent des **serveurs personnalisés** exclusivement pour leurs installations, sans les vendre ou les distribuer à l'extérieur. Une équipe de sécurité dédiée assure une surveillance continue 24h/24, 7j/7, garantissant des environnements parmi les plus sûrs pour héberger vos données.

Pour garantir la **continuité des opérations**, des mesures robustes sont en place, telles que le transfert automatique des données en cas d'incident majeur (incendie, panne de service) vers un autre centre de données, assurant ainsi une disponibilité sans interruption. Grâce à des **générateurs de secours** et à une certification ISO 22301:2019, ils garantissent une alimentation continue en cas de panne de courant.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

La **protection des données** est renforcée par la répartition des informations sur plusieurs serveurs géographiquement dispersés et la fragmentation aléatoire des données, ce qui empêche toute lecture non autorisée. Ils réalisent également des sauvegardes automatiques pendant l'utilisation, permettant une récupération rapide en cas d'incident.

Enfin, chaque **disque dur** est minutieusement suivi, et un processus rigoureux est appliqué pour détruire les disques en fin de vie, garantissant l'impossibilité d'accès aux données.

Les centres de données sont protégés par des **mesures de sécurité physiques avancées** : accès contrôlé par **authentification biométrique**, surveillance vidéo 24h/24 et équipes de sécurité sur place. Ils disposent aussi de **centres d'opérations de sécurité locaux et régionaux** pour surveiller et répondre aux incidents dans le monde entier, accompagnés d'une gestion proactive des risques et de tests de sécurité réguliers.

Pour plus d'information : https://www.google.com/about/datacenters/data-security/

Locaux Eurécia

Pour garantir la protection des informations et des infrastructures critiques, l'accès aux différents sites de l'entreprise est restreint grâce à un système de contrôle d'accès par badge, permettant de limiter l'entrée aux seules personnes autorisées et de tracer les visites. Par ailleurs, un système de vidéo protection est déployé afin de surveiller en continu les zones sensibles et de renforcer la sécurité des installations. Les locaux sont également protégés par un système d'alarme et de télésurveillance en dehors des horaires d'ouverture.

Les salles serveurs et les locaux hébergeant des équipements réseaux sont soumis à des mesures de protection renforcées. Ils sont verrouillés en permanence et leur accès est restreint aux seules personnes habilitées. Pour garantir un niveau de sécurité optimal, ces espaces critiques sont protégés par des serrures à code ou à clé, empêchant tout accès non autorisé.

Ces dispositifs s'inscrivent dans la démarche globale de sécurité d'Eurécia et assurent la confidentialité, l'intégrité et la disponibilité des actifs informationnels hébergés au sein de l'entreprise.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

eurécia

Sécurité des systèmes et applications

Développement sécurisé

Nous mettons un accent particulier sur le **développement sécurisé** afin de minimiser les vulnérabilités dans le code et garantir la sécurité de nos applications et des données des utilisateurs.

Formations aux développeurs

Nous organisons régulièrement des **formations sur la cybersécurité destinée** à nos tous nos collaborateurs, et des formations plus avancées aux développeurs. Ces formations couvrent les meilleures pratiques en matière de codage sécurisé, la gestion des vulnérabilités courantes et la mise en œuvre de solutions pour prévenir les risques liés aux attaques telles que les injections SQL, les failles XSS ou CSRF. Ces sessions sont conçues pour sensibiliser les équipes aux enjeux de sécurité tout au long du cycle de développement.

Sécurité par design

La sécurité est **intégrée dès la conception** de chaque solution. Dès la phase de planification, nous appliquons une approche "security by design", ce qui signifie que la sécurité est prise en compte à chaque étape du développement. Cela inclut la mise en place de mécanismes de contrôle d'accès robustes, de validation des entrées et de gestion stricte des permissions, afin de limiter les risques de vulnérabilités dans le produit final.

Gestion des droits des utilisateurs

Afin de garantir la **protection des données**, notre solution est conçue pour être **restrictive par défaut**. Aucun utilisateur n'a de droits d'accès initiaux. Ce sont nos clients qui définissent précisément qui peut accéder à quoi et quels droits sont attribués à chaque utilisateur. Cela permet d'assurer que l'accès aux données sensibles est strictement contrôlé et qu'aucun droit n’est accordé par défaut.

Ces mesures, combinées à des pratiques de développement rigoureuses, assurent une **protection continue** des systèmes et des données, tout en permettant à nos clients de garder un contrôle total sur l'accès et la gestion des informations sensibles.

Mises à jour et gestion des vulnérabilités

Nous avons mis en place des **procédures robustes** pour la gestion des mises à jour de sécurité et l’identification des vulnérabilités, afin de garantir la sécurité de nos applications.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Nous utilisons **DependencyTrack** pour effectuer une **veille continue sur les dépendances** et identifier rapidement les vulnérabilités potentielles dans nos bibliothèques et composants tiers. Cet outil nous permet de suivre en temps réel les mises à jour de sécurité et de réagir rapidement.

De plus, **Sonar** génère des **rapports de sécurité** détaillés, permettant de détecter les failles dans le code source et de les corriger immédiatement. Ces rapports sont essentiels pour une intervention rapide sur les vulnérabilités identifiées.

Enfin, nous appliquons des **mises à jour de sécurité régulières** pour garantir que notre logiciel et ses dépendances restent protégés contre les menaces émergentes.

Ces processus assurent une gestion proactive des vulnérabilités et une **sécurité continue** des systèmes d'Eurécia.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

eurécia

Gestion des Incidents de Sécurité

Disponibilité

Eurécia s'engage pleinement à garantir une **disponibilité optimale** du logiciel tout au long de l'année, assurant un accès **24 heures sur 24, 7 jours sur 7**, avec un objectif de **disponibilité (SLA) de 99,7%**. Cet engagement s'inscrit dans notre démarche de **haute disponibilité**, visant à offrir une solution stable et fiable à nos utilisateurs tout au long de l'année, y compris lors des périodes de forte sollicitation.

Nous mettons en place des **mesures de sécurité renforcées** et des protocoles de monitoring constants pour anticiper et répondre rapidement à tout incident pouvant affecter la continuité de service. Ces actions visent à maintenir une **stabilité élevée** de notre infrastructure, garantissant que le logiciel demeure accessible et fonctionnel à tout moment, tout en minimisant les risques de perturbation. Cette disponibilité est assurée, sous réserve des interventions de maintenance préventive, que nous nous engageons à effectuer exclusivement pendant les heures creuses, lorsque l'utilisation du logiciel est minimale, afin de minimiser l'impact sur les utilisateurs.

Détection et réponse aux incidents

Pour assurer une détection efficace des incidents de sécurité et une réponse appropriée, Eurécia a mis en place un processus structuré en plusieurs étapes :

Un **plan de réponse aux évènements et incidents** a été mis en place. Il joue un rôle central dans la gestion de la sécurité du SIRH, notamment sur les aspects liés au RGPD, aux cybermenaces et aux obligations légales.

- Le Plan de Réponse aux Événements et Incidents définit les actions à entreprendre en cas d'incident impactant la sécurité, la disponibilité ou la conformité du SIRH. Il couvre les obligations légales (RGPD, réversibilité des données) ainsi que la gestion des cybermenaces et des crises opérationnelles.
- Le plan encadre plusieurs scénarios :
    - RGPD & droits des utilisateurs
    - Effacement et réversibilité des données
    - Processus de communication : protocoles internes et externes en cas d'incident impactant les utilisateurs ou la conformité réglementaire.
    - Phishing & cyberattaques
    - Gestion des violations de données
    - Ransomware & menaces critiques

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

- Le plan prévoit une procédure d'escalade définie avec les services adaptés, l'informatique, le support, le legal, la direction.
- Le plan fixe aussi un registre des incidents et actions correctives

Nous avons également identifié un **groupe pour la gestion de crise** :

- Cette équipe est dédiée à la réponse rapide et efficace aux incidents impactant le Système d'Information des Ressources Humaines (SIRH). Son rôle est d'assurer la continuité des opérations, de limiter les impacts et de coordonner les actions correctives.
- L'objectif est de détecter, évaluer et prioriser les incidents affectant le SIRH, coordonner la réponse à l'incident en mobilisant les ressources nécessaires (Legal, Informatique, Support, Comex), communiquer aux parties prenantes concernées les actions en cours et les mesures à prendre, documenter l'incident et analyser les causes pour éviter sa réapparition, mettre en place et suivre des plans d'action post-crise.
- En cas d'incident critique identifié, ce groupe s'active pour une communication et coordination de toutes les équipes.

Plan de continuité des activités (PCA)

Notre Plan de Continuité d'Activité (PCA) est conçu pour assurer la disponibilité et la résilience de nos services, même en cas d'incident majeur. Nous avons mis en place une infrastructure hautement disponible sur Google Cloud Platform (GCP), avec des bases de données et des fichiers configurés en Haute Disponibilité (HA) sur trois zones/datacenters dans la région Paris. Cette configuration garantit une redondance et une continuité de service maximales. Comme recommandé par la CNIL, nous testons tous les mois la restauration de nos sauvegardes. La capacité à assurer la continuité de service est vérifiée et assurée par GCP.

Plan de reprise d'activité (PRA)

En cas de perte totale d'une région (par exemple, Paris), le PRA est activé pour permettre une reprise rapide des activités depuis la région de secours, minimisant ainsi l'impact sur les services. Les données sont sécurisées et protégées par un chiffrement de niveau AES-256, et des sauvegardes sont effectuées deux fois par jour, avec une rétention sur 60 jours. Ces sauvegardes sont stockées dans plusieurs zones et répliquées en Belgique, ainsi que dans nos locaux à près de Toulouse, pour garantir leur disponibilité, même en cas de défaillance d'une zone ou région spécifique.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Le PRA inclut également un processus de restauration des données, avec des tests réguliers de l'efficacité du plan, conformément aux recommandations de la CNIL en matière de sécurité et de continuité des activités. Cela permet de s'assurer que les procédures sont bien fonctionnelles et adaptées aux besoins de l'entreprise. Nous effectuons ce test au moins 1 fois par an.

Enfin, les équipes sont formées et les rôles et responsabilités clairement définis afin de réagir rapidement et efficacement en cas de déclenchement du PRA.

Reporting d'incident

La gestion des incidents constitue un pilier essentiel pour garantir la continuité, la fiabilité et la qualité de nos services.
Les incidents potentiels englobent des problèmes de sécurité, des interruptions d'accès à notre solution, ainsi que des bugs fonctionnels impactant l'expérience utilisateur.
Lorsqu'un incident est détecté, il est immédiatement signalé au service support, qui procède à une première analyse. Cette étape permet de qualifier et de prioriser l'incident en fonction de sa gravité et de son impact. Une fois cette évaluation effectuée, l'incident est transmis aux équipes techniques R&D les mieux adaptées pour sa résolution.

Pour optimiser la gestion et le suivi des incidents, nous utilisons la solution Zendesk, qui s'appuie sur des processus définis selon la nature et la sévérité de chaque problème. Les objectifs de délais de résolution sont structurés selon les priorités suivantes :

- **Problème urgent** : résolution sous 24 heures,
- **Problème élevé** : résolution sous une semaine,
- **Problème normal** : résolution sous un mois,
- **Problème faible** : résolution sous six mois.

Bien que ces délais ne soient pas contractuels, ils constituent des objectifs internes permettant d'assurer une prise en charge rapide et efficace des incidents signalés. Ce processus garantit une meilleure transparence et renforce la confiance des utilisateurs dans la continuité de nos services.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Sensibilisation et Formation

Sensibilisation des employés

Chez Eurécia, nous sensibilisons tous les employés plusieurs fois par an aux enjeux de la sécurité de l'information. Cette sensibilisation se fait à travers des présentations, des sessions de formation et des envois de mails réguliers. L'objectif est de renforcer la culture de sécurité au sein de l'organisation en veillant à ce que chaque employé comprenne les bonnes pratiques, les risques potentiels et les mesures à adopter pour garantir la protection des données et des systèmes.

Formation continue en sécurité

Nous imposons des formations obligatoires à tous nos employés sur la sécurité informatique, en abordant les risques majeurs, les techniques courantes utilisées par les pirates et les actions préventives à mettre en place pour protéger nos systèmes d'information. Ces sessions visent à assurer que chaque collaborateur soit bien informé des menaces potentielles et comprenne l'importance de ses actions pour garantir la sécurité des données. Pour nos équipes techniques, nous allons au-delà en leur proposant des formations approfondies sur les techniques de hacking avancées, leur permettant ainsi de comprendre en détail les méthodes des attaquants. Cette approche leur offre une vision pragmatique des vulnérabilités afin de mieux anticiper et contrer les attaques, renforçant ainsi notre posture de sécurité globale.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Audits et Évaluations

Audits internes et externes

Nous effectuons des audits de pentest, de sécurité, d'analyse des méthodologies et de respect des règles et politiques de sécurité au moins tous les ans via des intervenants externes. Le comité (définit en 8.2) assure que les procédures et politique soit maîtrisées, appliquées et reflètent les actions d'Eurécia pour assurer la sécurité interne et externe.

Amélioration continue

Nous analysons les résultats obtenus lors des audits de sécurité et des évaluations des risques. Cela inclut l'identification des vulnérabilités, qu'elles soient techniques ou organisationnelles, ainsi que l'évaluation de l'impact potentiel de ces faiblesses sur la confidentialité, l'intégrité et la disponibilité des données traitées.

A partir de cette analyse, nous établissons un plan d'action clair et priorisé, en tenant compte de la criticité des problèmes identifiés et des ressources disponibles. Les changements mis en place sont adaptés à ces risques : renforcement des contrôles d'accès, formation, corrections des vulnérabilités techniques... Ce qui nous permet de garantir la résilience de l'organisation et la protection des données traitées.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Gouvernance de la Sécurité de l'Information

Rôles et responsabilités

Rôle / Responsabilité	Responsabilités principales	Responsable
DPO (Délégué à la protection des données)	- Pilote l'ensemble des sujets RGPD : audit, rédaction des documents obligatoires, contrôle des prestataires, gestion des demandes d'exercice des droits - Réalise le suivi via des mises à jour régulières pour intégrer l'évolution de votre activité ainsi que les exigences légales en matière de conformité - Assure que Eurécia respecte le RGPD et les obligations CNIL	Dipeeo
Responsable de la gestion des incidents	- Pilote le Plan de Réponse aux Incidents (cyberattaques, phishing, ransomwares, fuites de données) et active le Groupe Gestion de Crise en cas d'incident majeur. - Documente les incidents, assure le suivi des mesures correctives et coordonne la communication interne/externe en cas de crise.	VP Opération d'Eurécia
Administrateurs système et réseau	- Mettre en place et maintenir les protections techniques (firewalls, antivirus, etc.) - Contrôler les accès aux systèmes d'information et garantir l'intégrité des données - Assurer la gestion des configurations de sécurité et des mises à jour	CTO d'Eurécia

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Responsable de la formation et sensibilisation	- Développer des programmes de formation pour sensibiliser le personnel aux bonnes pratiques de sécurité - Organiser des sessions de formation et d'évaluation des connaissances en matière de sécurité.	Head of IT d'Eurécia

Politique de révision et d'approbation

Ce document de sécurité est révisé **au moins une fois par an**, ou plus fréquemment si des changements significatifs surviennent dans l'environnement technique, réglementaire ou organisationnel.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Conclusion

Engagement envers la sécurité

Eurécia s'engage fermement à protéger la sécurité, la confidentialité et l'intégrité des informations traitées dans le cadre de nos services SaaS. Nous respectons pleinement les exigences légales en matière de sécurité de l'information et de protection des données personnelles, notamment le Règlement Général sur la Protection des Données (RGPD) et les autres réglementations applicables.

Pour ce faire, nous mettons en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données, gérer les risques, contrôler les accès et assurer la traçabilité. Nous formons régulièrement nos collaborateurs à la cybersécurité et à la protection des données.

En cas d'incident de sécurité, nous avons des procédures pour identifier, notifier et résoudre rapidement toute violation, conformément aux exigences légales. Nous nous engageons à revoir régulièrement nos pratiques pour assurer une sécurité optimale et une conformité continue.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Annexes

Documentation de référence

Audit Pentest

ITrust
CYBERSECURITY AS A SERVICE

CERTIFICAT D'AUDIT EXTERNE

EURECIA

3 Chem. Des Cannelles, 31320 Castanet-Tolosan, France

Ce document est un certificat délivré suite à un audit de sécurité réalisé sur les sites Internet de Eurecia.

ITRUST certifie qu'un Audit externe Boite Noire et Boite Grise a été réalisé entre le 23/10/2023 et le 27/10/2023 depuis les locaux d'ITRUST à Toulouse. L'audit s'est basé sur les normes ISO 27001, RGS et OWASP.

À la suite de l'audit, le risque informatique global de menace a été considéré comme **MINEUR**.

Éléments d'interprétation :

MINEUR	Le risque sur le système d'information est faible et n'impose pas d'actions importantes.
NOTABLE	Le risque sur le système d'information est modéré. Des impacts, fonctionnels, financiers ou en image, peuvent être subis. Ce niveau nécessite des actions à moyen terme.
MAJEUR	Le risque sur le système d'information est majeur. Des impacts significatifs, fonctionnels, financiers, légaux ou en image, peuvent être subis. Ce niveau impose des actions à court terme.
CRITIQUE	Le risque sur le système d'information est critique. Des impacts considérables, fonctionnels, financiers, légaux ou en image, peuvent être subis. Ce niveau impose des actions immédiates ou un arrêt des services vulnérables.

Jean-Nicolas PIOTROWSKI – Président ITRUST

Signature

ITrust SA - Société anonyme - Capital de 619 975,50 Euros – SIRET : 493 754 204 00029 NAF, ex APE : 6202A - RCS/RM : Toulouse B 493754204 - Num TVA : FR68493754204

Label conformité RGPD

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

Dans le cadre de sa démarche de conformité et de transparence, Eurécia informe ses clients qu'elle est labellisée « conforme au RGPD » par Dipeeo, notre DPO externalisé. Cette reconnaissance nous a été attribuée par notre DPO externe indépendant, à la suite d'un audit rigoureux. Cette labellisation atteste de notre engagement fort en matière de protection des données personnelles. Elle garantit que vos informations sont traitées dans le strict respect du Règlement Général sur la Protection des Données. Nous intégrons cette exigence au cœur de nos processus métier.

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268

eurécia

Attestation désignation du DPO

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

DÉSIGNATION
N° DPO-148826

DÉSIGNATION D'UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES

ORGANISME DÉSIGNANT LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

N° SIREN	487820268
Nom de l'organisme	EURECIA
Nom du représentant légal	Monsieur Pascal GRÉMIAUX
Email du représentant légal	dpo@eurecia.com
Nom du contact CNIL	Monsieur Pascal GRÉMIAUX
Email du contact CNIL	dpo@eurecia.com
Adresse postale	3 CHE DES CANELLES 31320 CASTANET-TOLOSAN
Pays	FRANCE

DÉLÉGUÉ À LA PROTECTION DES DONNÉES DÉSIGNÉ

N° SIREN	897692315
Organisme désigné	DIPEEO
Nom du représentant légal	Monsieur Raphael BUCHARD
Nom personne en charge de la désignation	Monsieur Raphael BUCHARD
Date prise d'effet	12/07/2024
Téléphone professionnel	0159068185
Téléphone portable	0159068185
Email	dpo@dipeeo.com
Adresse postale	95 AVENUE DU PRESIDENT WILSON 93100 MONTREUIL
Pays	FRANCE

COORDONNÉES PUBLIQUES

Ces informations de contact permettent à toute personne de joindre le délégué facilement. La CNIL les tient à disposition du public dans des formats ouverts.

Adresse postale publique	A l'attention de DPO de Eurécia 3 Chemin des Canelles 31320 CASTANET-TOLOSAN FRANCE
Adresse électronique dédiée	dpo@eurecia.com

Les exigences relatives à la désignation d'un délégué à la protection des données (statut, fonction, missions, qualités professionnelles) sont définies aux articles 37 à 39 du règlement européen relatif à la protection des données personnelles (RGPD). Le non-respect de ces dispositions est passible de sanctions.

En savoir plus : https://www.cnil.fr/le-dpo

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Pour en savoir plus : https://www.cnil.fr/donnees-personnelles

3 chemin des Canelles
31320 Castanet-Tolosan

SIRET : 487 820 268 00083
RCS : Toulouse B 487 820 268

TVA Intracommunautaire :
FR88487820268