GUIDE SÉCURITÉ

Doxa

GUIDE SÉCURITÉ & COMPLIANCE - Doxa

Meilleures Pratiques de Protection des Données

Version 1.5 | Décembre 2025

1 SECTION 1 : SÉCURITÉ INFRASTRUCTURE

1.1 1.1 Architecture sécurité Doxa

Chiffrement en transit :

- Tous transferts via HTTPS TLS 1.2 minimum
- Certificats SSL validés (Let's Encrypt)
- Perfect Forward Secrecy activé
- Pas de downgrade à HTTP possible

Chiffrement au repos :

- Base données : AES-256 chiffrement
- Files uploads : AES-256 chiffrement
- Clés chiffrement stockées séparément (KMS)
- Pas clé universelle (compromission = 1 client, pas tous)

Infrastructure :

- Hébergement data centers Algérie (certifications TIER III/IV)
- Auto-scaling + load balancing
- DDoS protection via Cloudflare
- IDS/IPS (Intrusion Detection/Prevention)
- WAF (Web Application Firewall)
- Monitoring 24/7

Audits sécurité :

- Audits externes annuels (pen-testing)
- Bug bounty program (security.doxa.dz)

- SOC 2 Type II audit (pro/enterprise)
- ISO 27001 certification

1.2 1.2 Espace de travail isolement

Isolation données par workspace :

- Chaque espace travail = données séparées complètement
- Utilisateur A (workspace 1) ne peut pas voir workspace 2 même avec même email
- Database queries isolées par tenant
- Impossible data leakage entre clients même avec bug

Isolation réseau :

- Chaque workspace sur subnet séparé (logiquement)
- Règles firewall par workspace
- Rate-limiting par workspace

2 SECTION 2 : AUTHENTIFICATION & ACCÈS

2.1 2.1 Authentification utilisateur

Standard (tous) :

- Email + Password
- Min 8 caractères, 1 majuscule, 1 chiffre
- Password hashed via bcrypt (salt randomisé)
- Session cookies httpOnly (pas accès JavaScript)
- Expiration session 30 jours

2FA - Authentification Double Facteur (activable) :

- TOTP (Time-based OTP) via Google Authenticator, Microsoft Authenticator, Authy
- Backup codes générés (10 codes, single-use)
- SMS OTP NOT disponible (moins sécurisé)

SSO - Single Sign-On (Enterprise) :

- SAML 2.0
- OAuth 2.0 (Google, Microsoft)
- OpenID Connect
- Okta, Azure AD, Ping Identity compatible

2.2 2.2 Gestion permissions

Rôles & Permissions :

```
Propriétaire
   Accès complet + supprimer espace + facturation

Admin
   Gérer membres, paramètres, mais pas facturation

Éditeur (par projet)
   Créer/modifier/comenter dans projet assigné

Lecteur (par projet)
   Lecture seule

Invité (single project)
   Lecture seule + commentaires optionnel
```

Best practices permissions :

- Principe moindre privilège : donnez minimum accès requis
- Audit régulier qui a quels accès
- Révoquez accès immédiatement quand personne quitte

2.3 2.3 API security

API Keys :

- Générées par utilisateur (Paramètres → API)
- Format : `sk_live_[32 char random]`
- Jamais exposez clés (commit repos, client JavaScript)

- Rotez tous les 90 jours minimum

Rate-limiting :

- Pro : 1000 requêtes/heure par API key
- Enterprise : custom (négocié)
- Dépasse limit = réponse 429 Too Many Requests

Webhooks :

- HMAC-SHA256 signature sur chaque webhook
- Timestamp incluse (récente/ancienne)
- Vous vérifiez signature (code exemple fourni)
- Retry automatique si timeout (exponentiel backoff)

3 SECTION 3 : DONNÉES PERSONNELLES & CONFORMITÉ ALGÉRIENNE

3.1 3.1 Conformité Loi 25-11 & Loi 18-07

Si vous stockez données personnelles :

- Vous = Responsable de Traitement (décidez quelles données)
- Doxa = Sous-traitant (traite per instructions)
- ATD (Accord Traitement Données) disponible
- Conformité obligations Loi 25-11 & 18-07 (transparence, consentement, sécurité)

7 principes clés Loi 25-11 & 18-07 :

1. **Légalité :**
   - Base légale pour chaque traitement données
   - Exemples : consentement, contrat, obligation légale
   - Documentez base légale
2. **Transparence :**
   - Dites aux utilisateurs quelles données, quoi vous faites
   - Politique confidentialité accessible

- Clauses confidentialité visibles

3. **Limitation finalité :**
   - Données utilisées UNIQUEMENT pour purpose déclaré
   - Pas utilisation secondaire sans consentement
   - Exemple : données support ≠ marketing sans accord
4. **Exactitude :**
   - Données à jour et exactes
   - Permettre correction si incorrect
   - Supprimez données obsolètes
5. **Limitation durée :**
   - Gardez données aussi longtemps que nécessaire
   - Supprimez quand pas utiles
   - Définir politique rétention avant collecting
6. **Intégrité & Confidentialité :**
   - Protégez données (chiffrement, accès contrôlé)
   - Prévenez perte, destruction, accès non-autorisé
   - Plan réaction incidents
7. **Responsabilité :**
   - Documentez conformité (registre, audits)
   - DPD désigné (obligation Loi 25-11)
   - Notification incidents ANPDP (5 jours)

3.2 3.2 Droits des personnes (données subjects)

Droit d'accès (art. 32 Loi 18-07) :

- Personne peut demander : quelles données vous avez sur moi ?
- Vous DEVEZ répondre dans 14 jours
- Format : copie de données (ex : email, export CSV)

Droit rectification :

- Si données inexactes, correction doit être possible
- Exemple : email vieux → personne change à nouveau
- Vous faciliter (formulaire, self-service)
- Correction effectuée sous 10 jours

Droit suppression (“droit être oublié”) :

- Personne peut demander suppression données
- Vous devez supprimer (sauf exception : obligation légale, archive, etc.)
- Doxa : via “Supprimer compte” → données effacées 30j

Droit portabilité :

- Données format lisible (CSV, JSON, etc.)
- Facilite migration services autres
- Doxa : export disponible

Droit opposition :

- Personne peut s’opposer traitement données
- Exemple : pas marketing par email
- Vous respectez

3.3 3.3 Incident données & notification (Loi 25-11)

Si breach (données non-autorisées accédées) :

Doxa actions :

1. Investigation immédiate ($<$ 24h)
2. Containment (arrêter accès non-autorisé)
3. Notification ANPDP dans 5 jours (obligation Loi 25-11)
4. Notification utilisateurs affectés ($<$ 30j)
5. Rapport détaillé breach

Vos actions recommandées :

- Notifiez autorités algériennes (ANPDP) si sérieux

- Communiquez transparently à utilisateurs
- Prenez measures remediation

4 SECTION 4 : CONFORMITÉ SECTEURS SPÉCIFIQUES

4.1 4.1 Santé (Loi 18-11 - Algérie)

Loi 18-11 = Loi relative à la santé (Algérie, 2 juillet 2018)

Doxa standard = **PAS compatible données patients sensibles sans mesures renforcées**.

Si besoin données patients (DME, santé) :

- Enterprise plan uniquement
- Signature Accord Traitement Données (ATD) OBLIGATOIRE
- Coûts additionnels (devis custom)
- Conformité garantie : chiffrement, audit logs, notification incidents
- Secret médical OBLIGATOIRE (art. 24 Loi 18-11)

Non recommandé :

- Store identifiants patients sans ATD signé
- Patient records sensibles
- Protected Health Information (PHI) sans sécurité renforcée

4.2 4.2 Finance (PCI-DSS)

PCI-DSS = Payment Card Industry Data Security Standard

Niveau compliance Doxa : **Level 1** (passerelle paiement uniquement)

Résumé :

- Jamais stockez numéros cartes (credit card) dans Doxa
- Paiements passent prestataire certifié (PCI Level 1 compliant)
- Doxa ne voit jamais numéros cartes complets

OK :

- Stocker “Customer paid 50,000 DZD on 2025-01-15”

- Stocker facture (montant, date, items)

PAS OK :

- 4532-XXXX-XXXX-1234 numéro visible
- CVV stocké anywhere
- Track 1/2 data

4.3 4.3 Gouvernement & Transferts Internationaux

Contrats gouvernement / données sensibles :

- Vérifiez requirements avant utilisation
- Certification nationale possiblement requise
- Data residency Algérie OBLIGATOIRE (Loi 25-11 art. 45 bis)
- Enterprise peut négocier conformité stricte
- Contactez sales@doxa.dz pour feasibility

Transferts Internationaux (Loi 25-11 art. 45 bis 13-14) :

- Doxa data centers = Algérie (par défaut)
- Tout transfert données hors Algérie = approbation ANPDP PRÉALABLE
- L'ANPDP vérifie niveau protection adéquat du pays destination
- Exceptions : coopération judiciaire, commissions rogatoires

5 SECTION 5 : SÉCURITÉ ÉQUIPE & BONNES PRATIQUES

5.1 5.1 Mots de passe forts

Critères mot de passe fort :

- Min 12-16 caractères (plus = meilleur)
- Majuscules + minuscules + chiffres + symboles
- Pas mot dictionnaire courant
- Pas informations personnelles (nom, date naissance, etc.)
- Unique (pas réutiliser)

Exemples :

```
Faible      : password, 123456, alice2024
Bon         : Kj$9pL@2mQ!xRs8vB
Meilleur    : Tr0pic@lSunset#2024$Sky9zKp
```

5.2 5.2 Authentification 2FA

Fortement recommandé :

1. Paramètres profil → “Sécurité”
2. “Activer authentification 2FA”
3. Scannez QR code avec Google Authenticator/Authy
4. Entrez code (6 chiffres) pour confirmer
5. Sauvegardez codes de backup 10 (stockez sécurisé)

À chaque login :

- Email + password → code 2FA (depuis authenticator app)
- Biométrique optionnel si app mobile

5.3 5.3 Gestion accès utilisateurs

Pour admin/propriétaire :

- Audit régulier : qui est dans espace ?
- Supprimez collègues qui partent
- Changez permissions si responsabilités changent
- Recertification semestrielle recommandée (cochez boxes)

Processus offboarding :

1. Révokez accès jour départ
2. Téléchargez ses données (export)
3. Supprimez compte
4. Changez mots de passe partagés (ex : Slack intégration)

5.4 5.4 Monitoring & alertes

Activer notifications sécurité :

- Paramètres → “Notifications sécurité”

- Alerte nouveau login location
- Alerte IP nouvelle
- Alerte 2FA désactivé

Logs d'activité :

- Admins peuvent voir audit logs par user (Enterprise)
- Qui a accédé quand, quelle action
- Conservation 12 mois minimum

6 SECTION 6 : INCIDENTS SÉCURITÉ

6.1 6.1 Signaler breach/vulnérabilité

Découvrez faille sécurité ?

Email immédiatement : security@doxa.dz

Ne pas :

- Publier sur social media
- Partager publiquement avant patch
- Exploiter vulnérabilité
- Tester sur production sans autorisation

Faire :

- Description claire
- Steps pour reproduire
- Impact potentiel
- Données exemple si possible

Réponse :

- Confirmation dans 24h
- Patch dans 7 jours (critique) ou 30 jours (normal)
- Credit sécurité chercheur si découverte valide (bug bounty)

6.2 6.2 Response breach détecté

Si Doxa détecte intrusion :

1. **Isolate** → arrêter accès non-autorisé
2. **Investigate** → quelles données, depuis quand ?
3. **Notify** → ANPDP et vous (5 jours), affectés (30j)
4. **Remediate** → patch vulnérabilité, upgrade sécurité
5. **Document** → rapport incident complet

7 SECTION 7 : CHECKLIST SÉCURITÉ

7.1 Pour Propriétaire / Admin

Première configuration :

- [ ] Changez password fort (min 16 char)
- [ ] Activez 2FA (authenticator app)
- [ ] Configurez adresse billing correct
- [ ] Vérifiez authorized members

Mensuel :

- [ ] Revoyez qui a accès (Admin audit)
- [ ] Vérifiez aucune activité suspecte
- [ ] Confirmez integrations toujours utilisées
- [ ] Rotation API keys (90 jours min)

Trimestriel :

- [ ] Revoquer accès utilisateurs partis
- [ ] Audit logs review (Enterprise)
- [ ] Test disaster recovery (backup restoration)
- [ ] Mettre à jour données membres

Annuel :

- [ ] Security assessment (self ou tiers)

Update ATD si Loi 25-11 changes

Compliance check (Loi 18-11 si applicable, transfers data)

Recertification permissions

7.2 Pour tous les utilisateurs

Une fois :

Mot de passe fort changé

2FA activé

Politique confidentialité lue

Pas partager credentials

Régulier :

Logout après usage public

Ne pas laisser onglets ouvertes

Vérifier email phishing Doxa

Signaler activité suspecte

8 SECTION 8 : DISASTER RECOVERY

8.1 8.1 Backups Doxa

Backups automatiques :

- Quotidiens (1 backup/jour)
- Conservés 90 jours (rolling window)
- Testés régulièrement restoration
- Géographiquement distribués (fault tolerance, data centers Algérie)

Récupération :

- Perte accidentelle données $\leq$ 24h ? Contact support
- Data recovery possible jusqu'à 90j back
- Enterprise : restore point custom

8.2 8.2 Vos backups (recommandé)

Même si Doxa backup, export vos données :

1. Mensuel export : Paramètres → “Exporter données” → CSV/JSON
2. Archivez localement (encrypted external drive)
3. Test restauration annuel

Données critiques :

- Projets actifs (export tous les mois)
- Historique tickets support (archive annuel)
- Documents relatifs tâches (pièces jointes zip)

9 SUPPORT SÉCURITÉ

Questions sécurité ?

security@doxa.dz

Signaler vulnérabilité ?

security.doxa.dz (bug bounty)

Demande données (Loi 25-11 droit accès) ?

privacy@doxa.dz

Incident/Breach ?

emergency@doxa.dz (24h response)