

DHDP Infrastructure

The Platform v1.0 product has been developed, integrating DHDP's technical partners existing solutions into one. Refer to the "[DHDP Functionalities](#)" resource to learn more about Platform functionalities. DHDP continues technological development using end-user feedback, expertise of subject matter experts, and agile methodology to drive continuous platform improvements. By January 2026, from an infrastructure standpoint, DHDP will have achieved or continue working toward:

1. **Compliance with Industry Standards**
2. **Strong Data Encryption & Protection**
 - **End-to-end encryption** (AES-256) for data at rest and TLS 1.2+ for data in transit.
 - **De-identification** techniques to protect sensitive data.
 - **Strict data residency policies** ensuring compliance with provincial and institutional requirements.
3. **Robust Access Controls & Identity Management**
 - **Role-based access control (RBAC)** and **least privilege principles** to restrict data access.
 - **Multi-factor authentication (MFA)** for user accounts and privileged access.
4. **Continuous Monitoring & Threat Detection (IDPS and SIEM)**
 - 24/7 security monitoring and automated threat detection
5. **Secure Cloud Infrastructure & Data Governance**
 - **DHDP Orchestrator** is hosted on a **highly secure cloud platform** (AWS, Azure) with built-in security controls.
 - **Regular security patching and vulnerability management**
 - **Comprehensive data governance framework** ensuring ethical data usage and regulatory compliance.
6. **Third-Party Risk Management & Secure Integrations**
 - **Vendor security assessments** to ensure third-party tools meet DHDP's security standards.
 - **Secure API integrations** with encryption and authentication mechanisms.
 - **Strict contract requirements** for data security and compliance with external parties.
7. **Regular Security Testing & Incident Response Preparedness**
 - **Incident response plan** with predefined protocols to handle security breaches.
 - **Data backup & disaster recovery** strategies ensuring data integrity and availability.

Infrastructure DHDP

Le produit v1.0 de la plateforme a été développé, intégrant les solutions existantes des partenaires techniques de DHDP en une seule. Reportez-vous à la ressource « [Fonctionnalités DHDP](#) » pour en savoir plus sur les fonctionnalités de la plateforme. DHDP poursuit son développement technologique en s'appuyant sur les retours des utilisateurs finaux, l'expertise d'experts en la matière et une méthodologie agile pour améliorer continuellement la plateforme. D'ici janvier 2026, d'un point de vue infrastructurel, DHDP aura atteint ou continuera à travailler pour :

- Conformité aux normes de l'industrie
- Chiffrement et protection des données
 - Chiffrement de bout en bout (AES-256) pour les données au repos et TLS 1.2+ pour les données en transit.
 - Techniques de désidentification pour protéger les données sensibles.
 - Politiques strictes de résidence des données garantissant la conformité aux exigences provinciales et institutionnelles.
- Contrôles d'accès et gestion des identités
 - Contrôle d'accès basé sur les rôles (RBAC) et principe du moindre privilège pour restreindre l'accès aux données.
 - Authentification multifacteur (MFA) pour les comptes utilisateurs et les accès privilégiés.
- Surveillance continue et détection des menaces (IDPS et SIEM)
 - Surveillance de la sécurité 24h/24 et 7j/7 et détection automatisée des menaces
- Infrastructure cloud sécurisée et gouvernance des données
 - DHDP Orchestrator est hébergé sur une plateforme cloud hautement sécurisée (AWS, Azure) avec des contrôles de sécurité intégrés.
 - Mise à jour régulière des correctifs de sécurité et gestion des vulnérabilités
 - Cadre complet de gouvernance des données garantissant une utilisation éthique des données et la conformité réglementaire.
- Gestion des risques liés aux tiers et intégrations sécurisées
 - Évaluations de la sécurité des fournisseurs pour s'assurer que les outils tiers répondent aux normes de sécurité de DHDP.
 - Intégrations d'API sécurisées avec des mécanismes de chiffrement et d'authentification.
- Exigences contractuelles strictes en matière de sécurité des données et de conformité avec les parties externes.
- Tests de sécurité réguliers et préparation à la réponse aux incidents
 - Plan de réponse aux incidents avec des protocoles prédéfinis pour gérer les failles de sécurité.
 - Stratégies de sauvegarde des données et de reprise après sinistre garantissant l'intégrité et la disponibilité des données.