Protection Ordinateur AS
Computer Protection AS

PROTECTION ORDINATEUR AS

Professional IT Services, Computer Repair, Cybersecurity & Web Solutions
514-970-5667 | support@protectionordinateuras.com |
www.protectionordinateurAS.com

Choose your language **English** / Choisissez votre langue **French**

What Customers Can Expect

Protection Ordinateur AS helps Québec businesses simplify technology by combining software delivery, managed IT, and security operations under one bilingual team. Instead of coordinating multiple vendors for infrastructure, Microsoft 365, cybersecurity, support, and application delivery, clients work with one partner responsible for the full process from discovery to launch and ongoing support.

This brief explains how a typical engagement works, what happens at each phase, what your team should prepare, and what you can expect from us before kickoff, during rollout, and after go-live.

What this playbook is for

This document is designed for organizations that want:

- managed IT with clearer accountability,
- a more secure Microsoft 365 and endpoint environment,
- better internal systems and workflows,
- a web or mobile app delivered with operational support in mind,
- and one bilingual Québec-based partner that can stay involved after launch.

What customers can expect

When you work with Protection Ordinateur AS, you can expect a direct, structured process.

You will know what is being reviewed, what is being prioritized, what is being built, what is being secured, and what happens after delivery. The goal is not just to ship technology. The goal is to leave you with a cleaner operating model, fewer surprises, and a support structure that continues after implementation. This reflects the company's stated model of fewer handoffs, clearer accountability, and practical engineering delivered in English and French.

Step 1 — Audit & Discovery

Objective

Understand the current environment, identify risks and bottlenecks, and define what success looks like.

What happens

We begin with a discovery phase. Depending on the engagement, that can include a review of your current IT environment, Microsoft 365 setup, network posture, backup status, endpoint management, security controls, or the product and workflow requirements behind a new application.

For software projects, we look at user flows, business goals, technical constraints, reporting needs, access control, and how the system should support day-to-day operations. For managed IT and security engagements, we review the practical foundation: devices, users, permissions, patching, support issues, Wi-Fi/network health, backup readiness, and the current risk profile. This matches the service scope described across your managed IT, networking, cybersecurity, and app pages.

What the client provides

- Current pain points and goals
- Key contacts and decision makers
- Existing systems, vendors, and tools
- Access to relevant documentation or screenshots
- A rough idea of priorities, deadlines, or budget range

What the client receives

- A high-level findings summary
- Early risk and opportunity notes
- Initial recommendations
- A clearer view of scope and next steps

What to expect

This phase is meant to reduce confusion. It gives both sides a shared understanding before time is spent building or changing anything.

Step 2 — Roadmap & Sprint Planning

Objective

Turn findings into a practical action plan.

What happens

Once the audit is complete, we define the recommended path forward. This is where the engagement becomes structured.

For managed IT, that may mean identifying which systems need stabilization first, what should be standardized, which controls should be improved, and what support coverage should look like. For app delivery, it means translating business needs into a roadmap with clear priorities, milestones, features, rollout expectations, and launch criteria.

This phase is especially important for organizations that have inherited messy infrastructure, technical debt, or an app that needs improvement instead of a full rebuild. Your site explicitly positions this as part of the process: some projects start from zero, others start with inherited systems or controlled rebuilds.

What the client receives

- Recommended scope
- Priority order
- Sprint or rollout plan
- Dependencies and risks
- Suggested implementation sequence

What to expect

You should come out of this stage knowing:

- what happens first,
- what can wait,
- what will require internal input,
- and what success will look like at go-live.

Step 3 — Build, Implement & Roll Out

Objective

Execute the work in focused stages without losing visibility or control.

What happens

This is the delivery phase.

For IT engagements, this can include endpoint setup, patching baselines, Microsoft 365 administration, network improvements, backup configuration, user support setup, and operational standardization. For software engagements, this can include UX refinement, development, integrations, client portals, internal tools, mobile features, workflow automation, reporting dashboards, testing, and release preparation. These service categories are all described on your live site.

We work in a way that keeps progress understandable. Clients should never feel like work is happening in a black box. The process is designed to keep teams aligned while avoiding unnecessary complexity.

What the client can expect during rollout

- Clear communication on progress
- Defined milestones
- Focused execution instead of random changes
- Escalation when decisions are needed
- Practical adjustments when priorities shift

What matters here

The point of rollout is not just to “finish the work.” It is to leave the environment more stable, more usable, and easier to support afterward.

Step 4 — Security, Hardening & Risk Reduction

Objective

Make security part of delivery, not an afterthought.

What happens

Security is built into the implementation process. Protection Ordinateur AS positions security by default across its practice, including endpoint protection, Microsoft 365 hardening, phishing risk reduction, policy improvements, monitoring, incident response support, executive reporting, and Law 25 readiness support for Québec organizations.

That means a proper rollout does not stop at “it works.” It also considers:

- who has access,
- what should be logged,
- how devices are protected,
- whether backups are reliable,
- how identities and sessions are managed,
- and what documentation is needed to support compliance or future support.

For app projects, this can also include secure sessions, controlled permissions, safer file handling, and preparation for operational support after launch. For IT projects, this can include EDR, policy hardening, support procedures, and clearer documentation.

What the client receives

- A more secure baseline
- Reduced day-to-day risk
- Better visibility into controls
- Documentation or reporting where appropriate
- A stronger foundation for ongoing support

What to expect

Security work should feel practical, not theatrical. The goal is to reduce risk without making operations harder than they need to be.

Step 5 — Launch, Support & Ongoing Ownership

Objective

Make sure the work stays useful after delivery.

What happens

After launch or implementation, support matters just as much as build quality. Protection Ordinateur AS presents itself as a bilingual Québec team offering same-day email intake, escalation paths for urgent issues, and ongoing operational support rather than one-time delivery only.

This stage can include:

- post-launch support,
- issue triage,
- user assistance,
- small adjustments,
- monitoring and maintenance,
- roadmap follow-up,
- and long-term operational ownership where needed.

For many clients, this is where the value becomes most obvious. Instead of being handed off after go-live, they continue working with the same partner who already understands the environment and the original goals.

What the client can expect

- Continued communication
- Ongoing support options
- Faster issue resolution
- A known point of contact
- Less vendor handoff and less re-explaining

Typical client journey

Before kickoff

You bring the context: goals, frustrations, existing tools, and what is not working.

During discovery

We assess the environment and identify what needs attention first.

During planning

We turn that into a roadmap and define what should be done in what order.

During execution

We implement in focused stages with communication and accountability.

Before launch

We review readiness, security, and support expectations.

After go-live

We stay available for support, follow-up, and continuous improvement.

Who is involved

Your team

Your team helps define priorities, answer business questions, approve decisions, and provide internal context that technical work alone cannot reveal.

Our team

We handle the technical review, planning, implementation, hardening, and support structure according to the agreed scope.

Shared responsibility

The best results happen when priorities are clear, approvals are timely, and the process is treated as a partnership instead of a last-minute handoff.

Communication expectations

Clients should expect direct communication, realistic recommendations, and plain-language explanations.

That matters because your site repeatedly emphasizes practical engineering, direct ownership, bilingual delivery, and reducing unnecessary process. The playbook should reflect that tone: clean, accountable, and understandable to business owners and operators, not just technical teams.

What that looks like in practice:

- clear next steps,
- honest scope discussions,
- early identification of risks,
- no unnecessary jargon,
- and no confusion about who owns what.

What makes this different

Many businesses end up juggling separate vendors for support, security, Microsoft 365, networking, and software delivery.

Protection Ordinateur AS is positioned around a different model: one partner that can review the environment, improve the technology stack, support the users, secure the foundation, and stay involved once the project is live. That is a major theme across your About, managed IT, app development, and cybersecurity pages.

This means customers can expect:

- fewer handoffs,
- clearer accountability,

- stronger continuity,
- and better alignment between technology decisions and business operations.

Best fit for this playbook

This model is a strong fit for:

- Québec SMEs that want one accountable partner,
- organizations replacing reactive IT support,
- teams launching or rebuilding internal tools or customer portals,
- businesses that need stronger Microsoft 365 or endpoint security,
- and clients that want support after delivery instead of being left on their own.

Closing note

A strong project does not begin with a rushed quote or a random task list. It begins with clarity.

This playbook exists so your team can understand the process before kickoff: what will be reviewed, how priorities will be set, how rollout will happen, how security will be handled, and what support will look like once the work is live.

Audit → Plan → Build → Secure → Support
That is the operating model.

À quoi les clients peuvent s'attendre avec Protection Ordinateur AS

Protection Ordinateur AS aide les entreprises du Québec à simplifier leur technologie en réunissant sous une même équipe bilingue la livraison d'applications, l'informatique gérée et la cybersécurité.

Au lieu de coordonner plusieurs fournisseurs pour l'infrastructure, Microsoft 365, la sécurité, le soutien technique et le développement logiciel, les clients travaillent avec un seul partenaire responsable de l'ensemble du processus, de la découverte initiale jusqu'au lancement et au soutien continu.

Ce guide explique comment se déroule un mandat typique, ce qui se passe à chaque étape, ce que votre équipe doit préparer et à quoi vous pouvez vous attendre avant le démarrage, pendant le déploiement et après la mise en production.

À quoi sert ce guide

Ce document s'adresse aux organisations qui veulent :

- une informatique gérée avec une meilleure imputabilité,
- un environnement Microsoft 365 et postes de travail plus sécuritaire,
- de meilleurs systèmes internes et flux de travail,
- un site web ou une application mobile livrée avec une vraie logique de support,
- et un seul partenaire bilingue au Québec capable de rester impliqué après le lancement.

Ce que les clients peuvent attendre

Quand vous travaillez avec Protection Ordinateur AS, vous pouvez vous attendre à un processus direct et structuré.

Vous saurez ce qui est analysé, ce qui est priorisé, ce qui est construit, ce qui est sécurisé et ce qui se passe après la livraison. L'objectif n'est pas seulement de livrer une technologie. L'objectif est de vous

laisser avec un environnement plus clair, moins de surprises et une structure de soutien qui continue après l'implantation.

Étape 1 — Audit et découverte

Objectif

Comprendre l'environnement actuel, repérer les risques et les blocages, et définir ce qu'est une réussite pour le projet.

Ce qui se passe

Nous commençons par une phase de découverte. Selon le mandat, cela peut inclure une révision de votre environnement TI actuel, de votre configuration Microsoft 365, de votre posture réseau, de vos sauvegardes, de la gestion de vos postes de travail, de vos contrôles de sécurité, ou encore des besoins opérationnels derrière une nouvelle application.

Pour les projets logiciels, nous analysons les parcours utilisateurs, les objectifs d'affaires, les contraintes techniques, les besoins en rapports, les accès et la façon dont le système doit soutenir les opérations au quotidien. Pour les mandats de services gérés et de sécurité, nous examinons la base pratique : appareils, utilisateurs, permissions, mises à jour, incidents de support, qualité du Wi-Fi et du réseau, état des sauvegardes et profil de risque actuel.

Ce que le client fournit

- Les irritants actuels et les objectifs
- Les personnes responsables et décideurs
- Les systèmes, outils et fournisseurs en place
- L'accès à la documentation pertinente ou à des captures d'écran

- Une idée générale des priorités, échéances ou budget

Ce que le client reçoit

- Un résumé initial des constats
- Les premiers risques et opportunités observés
- Des recommandations de départ
- Une meilleure compréhension de la portée et des prochaines étapes

À quoi s’attendre

Cette étape sert à réduire le flou. Elle permet aux deux parties de partir avec une compréhension commune avant de commencer à construire ou à modifier quoi que ce soit.

Étape 2 — Feuille de route et planification des sprints

Objectif

Transformer les constats en plan d’action concret.

Ce qui se passe

Une fois l’audit terminé, nous définissons la meilleure façon d’avancer. C’est ici que le mandat devient structuré.

Pour l'informatique gérée, cela peut vouloir dire identifier quels systèmes doivent être stabilisés en priorité, ce qui doit être standardisé, quels contrôles doivent être renforcés et à quoi doit ressembler le soutien. Pour la livraison d'applications, cela signifie transformer les besoins d'affaires en une feuille de route avec des priorités claires, des étapes, des fonctionnalités, des attentes de déploiement et des critères de lancement.

Cette phase est particulièrement importante pour les organisations qui ont hérité d'une infrastructure désordonnée, d'une dette technique ou d'une application qui a besoin d'être améliorée au lieu d'être reconstruite au complet.

Ce que le client reçoit

- Une portée recommandée
- L'ordre de priorité
- Un plan de sprint ou de déploiement
- Les dépendances et risques
- Une séquence d'implantation suggérée

À quoi s'attendre

À la fin de cette étape, vous devriez savoir :

- ce qui vient en premier,
- ce qui peut attendre,
- ce qui demandera une participation interne,
- et à quoi ressemblera une mise en production réussie.

Étape 3 — Construction, implantation et déploiement

Objectif

Exécuter le travail en étapes ciblées sans perdre la visibilité ni le contrôle.

Ce qui se passe

C'est la phase de livraison.

Pour les mandats TI, cela peut inclure la configuration de postes, les bases de mises à jour, l'administration Microsoft 365, les améliorations réseau, la configuration de sauvegardes, la mise en place du support utilisateur et la standardisation des opérations. Pour les mandats logiciels, cela peut inclure l'amélioration de l'expérience utilisateur, le développement, les intégrations, les portails clients, les outils internes, les fonctions mobiles, l'automatisation, les tableaux de bord, les tests et la préparation au lancement.

Nous travaillons d'une façon qui garde le progrès compréhensible. Les clients ne devraient jamais avoir l'impression que le travail se fait dans une boîte noire. Le processus est conçu pour garder tout le monde aligné tout en évitant la complexité inutile.

Ce que le client peut attendre pendant le déploiement

- Une communication claire sur l'avancement
- Des jalons définis
- Une exécution ciblée au lieu de changements aléatoires
- Une remontée rapide quand une décision est nécessaire
- Des ajustements pratiques lorsque les priorités changent

Ce qui compte ici

Le but du déploiement n'est pas seulement de "terminer le travail". Le but est de laisser l'environnement plus stable, plus utile et plus simple à soutenir par la suite.

Étape 4 — Sécurité, durcissement et réduction des risques

Objectif

Faire de la sécurité une partie intégrée de la livraison, et non une réflexion de dernière minute.

Ce qui se passe

La sécurité est intégrée au processus d'implantation.

Cela signifie qu'un bon déploiement ne s'arrête pas à "ça fonctionne". Il tient aussi compte :

- de qui a accès à quoi,
- de ce qui doit être journalisé,
- de la façon dont les appareils sont protégés,
- de la fiabilité des sauvegardes,
- de la gestion des identités et des sessions,
- et de la documentation nécessaire pour le soutien futur ou la conformité.

Pour les projets d'application, cela peut aussi inclure la gestion sécurisée des sessions, des permissions contrôlées, une meilleure gestion des fichiers et une préparation au soutien opérationnel après le lancement. Pour les mandats TI, cela peut inclure l'EDR, le durcissement des politiques, les procédures de support et une meilleure documentation.

Ce que le client reçoit

- Une base plus sécuritaire

- Une réduction du risque au quotidien
- Une meilleure visibilité sur les contrôles
- De la documentation ou des rapports, au besoin
- Une fondation plus solide pour le soutien continu

À quoi s’attendre

Le travail de sécurité doit être concret, pas théâtral. L’objectif est de réduire le risque sans compliquer inutilement les opérations.

Étape 5 — Lancement, soutien et continuité

Objectif

S’assurer que la solution demeure utile après la livraison.

Ce qui se passe

Après le lancement ou l’implantation, le soutien est aussi important que la qualité de la construction.

Cette étape peut inclure :

- le soutien post-lancement,
- le triage des incidents,
- l’aide aux utilisateurs,
- les petits ajustements,
- la surveillance et la maintenance,
- le suivi de la feuille de route,
- et la prise en charge à plus long terme lorsque nécessaire.

Pour plusieurs clients, c'est là que la valeur devient la plus évidente. Au lieu d'être laissés à eux-mêmes après la mise en production, ils continuent avec le même partenaire qui connaît déjà l'environnement et les objectifs du projet.

Ce que le client peut attendre

- Une communication continue
- Des options de soutien à long terme
- Une résolution plus rapide des problèmes
- Un point de contact connu
- Moins de transferts entre fournisseurs et moins de répétition

Le parcours typique du client

Avant le démarrage

Vous apportez le contexte : objectifs, frustrations, outils existants et ce qui ne fonctionne pas.

Pendant la découverte

Nous analysons l'environnement et identifions ce qui doit être traité en premier.

Pendant la planification

Nous transformons cela en feuille de route et nous définissons l'ordre des priorités.

Pendant l'exécution

Nous implantons le travail par étapes ciblées avec communication et imputabilité.

Avant le lancement

Nous validons l'état de préparation, la sécurité et les attentes en matière de soutien.

Après la mise en production

Nous demeurons disponibles pour le soutien, les suivis et l'amélioration continue.

Qui est impliqué

Votre équipe

Votre équipe aide à définir les priorités, répond aux questions d'affaires, approuve certaines décisions et fournit le contexte interne qu'un travail purement technique ne peut pas révéler.

Notre équipe

Nous prenons en charge l'analyse technique, la planification, l'implantation, le durcissement et la structure de soutien selon la portée convenue.

Une responsabilité partagée

Les meilleurs résultats arrivent lorsque les priorités sont claires, les approbations sont données à temps et que le projet est traité comme un partenariat plutôt qu'un simple transfert de tâches.

Les attentes en communication

Les clients doivent s'attendre à une communication directe, à des recommandations réalistes et à des explications en langage clair.

Concrètement, cela veut dire :

- des prochaines étapes claires,
- des discussions honnêtes sur la portée,
- l'identification rapide des risques,
- peu de jargon inutile,
- et aucune confusion sur qui est responsable de quoi.

Ce qui rend cette approche différente

Beaucoup d'entreprises se retrouvent à gérer différents fournisseurs pour le support, la sécurité, Microsoft 365, le réseau et le développement logiciel.

Protection Ordinateur AS repose sur un modèle différent : un seul partenaire capable d'analyser l'environnement, d'améliorer l'écosystème technologique, de soutenir les utilisateurs, de sécuriser la fondation et de rester impliqué après le lancement.

Cela veut dire que les clients peuvent s'attendre à :

- moins de transferts,
- une meilleure imputabilité,
- une continuité plus forte,
- et un meilleur alignement entre les décisions technologiques et les opérations d'affaires.

Pour qui ce playbook est le mieux adapté

Ce modèle convient particulièrement :

- aux PME québécoises qui veulent un seul partenaire responsable,
- aux organisations qui veulent remplacer un support TI réactif,
- aux équipes qui lancent ou reconstruisent des outils internes ou des portails clients,
- aux entreprises qui ont besoin d'un meilleur encadrement Microsoft 365 ou d'une sécurité renforcée,
- et aux clients qui veulent du soutien après la livraison plutôt qu'un simple projet ponctuel.

Mot de la fin

Un bon projet ne commence pas par une soumission improvisée ou une liste de tâches désordonnée. Il commence par de la clarté.

Ce playbook existe pour que votre équipe comprenne le processus avant le démarrage : ce qui sera analysé, comment les priorités seront définies, comment le déploiement se fera, comment la sécurité sera gérée et à quoi ressemblera le soutien une fois le travail en production.

Audit → Planification → Construction → Sécurité → Soutien
Voilà le modèle.