

# IT Book

## Version 09.2024



Septembre 2024

# Introduction

L'IT Book est produit par la DSI Pôle de VINCI Construction en collaboration avec les DSI de division. Il définit les services SI, les règles associées et bonnes pratiques à appliquer par toutes les équipes IT.  
La DSI Pôle est responsable de sa mise à jour.

## Dans ce cadre, le présent catalogue définit :

- La liste des services IT disponibles
- Les règles et les bonnes pratiques
- Les contacts et responsables IT
- Les indicateurs de performance

## À qui est-il destiné ?

Le catalogue est un document à destination de tous les IT managers des divisions, des pays et des délégations du pôle VINCI Construction.

Ce document est également accessible à tous les collaborateurs VINCI Construction à titre informatif.



### Important :

L'IT Book décrit les différentes configurations disponibles des services proposés niveau Pôle.

Pour des réseaux techniques ou stratégies métiers, ces configurations peuvent varier d'une Division et périmètre à l'autre.

Cela sera explicitement indiqué lorsque possible, mais la richesse des contextes peut présenter parfois une différence avec l'enjeux de synthèse que vise à adresser l'IT Book.

## Légende

	Nouveau
	Travail en cours

# Sommaire



# Responsables DSi Pôle

	Fiche	Responsables
Poste de travail	<u>1.1 Matériel</u>	V. DAVID
	1.2 Poste de travail	
	<u>1.2.1 PC management</u>	C. GASNIER
	<u>1.2.2 Mobile management</u>	C. GASNIER
	<u>1.3 Virtual Private Network (VPN)</u>	M. AZERAD
	1.4 Système de messagerie	
	<u>1.4.1 Messagerie Outlook</u>	L. BENOIT
Réseau	<u>1.4.2 Sécurité de la messagerie</u>	L. BENOIT
	<u>1.4.3 Gestion des courriers indésirables</u>	L. BENOIT
	<u>1.5 Liste de diffusion</u>	L. BENOIT
Serveurs & Cloud	<u>1.6 Téléphonie Teams</u>	L. BENOIT
	<u>1.7 Antivirus</u>	M. AZERAD
Identité & Référentiel	<u>2.1 Réseaux disponibles</u>	M. AZERAD
	<u>2.2 Wi-Fi</u>	M. AZERAD
	<u>3.1 Cloud Privé</u>	W. DALLEAU
	<u>3.2 Cloud public</u>	W. DALLEAU
	<u>3.3 Archivage</u>	P. D'AGOSTINO
	<u>3.4 Scan de vulnérabilité</u>	M. AZERAD
Support	<u>4.1 Licences utilisateurs (bundles)</u>	L. BENOIT
	<u>4.2 Licences à la carte</u>	L. BENOIT
	<u>4.3 Comptes standards et comptes à privilèges</u>	L. BENOIT
	<u>4.4 Authentification forte (MFA)</u>	T. PREVOT
	<u>4.5 Accès conditionnels</u>	JA. DE NICOLAY
	<u>4.6 Référentiel d'architecture</u>	A. PEUREUX
Organisation	<u>5.1 Accompagnement sur les outils collaboratifs et bureautiques</u>	C. HOULES
	<u>5.2 Accompagnement du changement</u>	C. LEJEUNE / J. ASTAR
	<u>5.3 Négociation et suivi de contrat IT</u>	V. DAVID
	<u>5.4 Offre UX</u>	T. GREBERT
	<u>5.5 Sécurité dans les projets IT</u>	G. RIVET
	<u>6.1 Ressources IT</u>	T. MELIN
	<u>6.2 UNITY Service book</u>	R. BLACKIE
	<u>6.3 Support utilisateurs</u>	J. DA FONSECA
	<u>6.4 IT Service Management</u>	J. GUITARD
	<u>6.5 Facturation des coûts IT</u>	V. DAVID

**NEW**

# QUOI DE NEUF ?

V04.2024

## Transversal

- UPDATE** All - Réorganisation des catégories  
- Cybersécurité répartie dans les chapitres dédiés

## 1. Poste de travail

<b>UPDATE</b>	1.1	Matériel	Précisions sur la durée de vie des PC
<b>UPDATE</b>	1.2.1	PC Management	UNITY obtient les droits d'administration et la conformité des postes de travail
<b>UPDATE</b>	1.4.1	Messagerie Outlook	Règles pour les noms d'affichage et détails sur les quotas
<b>UPDATE</b>	1.4.3	Gestion des courriers indésirables	Ajout d'un diagramme sur la conformité
<b>NEW</b>	1.7	Antivirus	Présentation de l'EDR et de la PPE

## 2. Réseau

<b>NEW</b>	2.1	Réseaux disponibles	Types de connectivités et différentes technologies
<b>NEW</b>	2.2	Wi-Fi	Présentation des différents types de réseaux Wi-Fi disponibles

## 3. Serveurs & Cloud

<b>UPDATE</b>	3.1	Archivage	Changement du navigateur web et de la solution de gestion des documents
---------------	-----	-----------	---

## 4. Identité & référence

<b>UPDATE</b>	4.1	Licences utilisateurs (Bundles)	Mise à jour des noms de groupes et précision sur les quotas de boîtes aux lettres Ajout d'informations sur le stockage des utilisateurs
<b>UPDATE</b>	4.2	Licences à la carte	Mise à jour des noms de groupes
<b>UPDATE</b>	4.3	Comptes standards et compte à priviléges	- utilisation de mots de passe forts - processus de suppression des comptes privilégiés non utilisés
<b>NEW</b>	4.5	Accès conditionnels	Stratégies matérielles et de cybersécurité
<b>NEW</b>	4.6	Référentiel d'architecture	Présentation de la solution et de l'accès

## 5. Support

<b>NEW</b>	5.5	Sécurité dans les projets IT	La cybersécurité dans le cycle de vie des solutions et outils informatiques
------------	-----	------------------------------	---

## 6. Organisation

<b>UPDATE</b>	6.1	Ressources IT	Ajout d'un lien vers les coûts informatiques
<b>UPDATE</b>	6.2	UNITY Services Book	Lien vers le Service Book
<b>UPDATE</b>	6.3	Support utilisateurs	Ajout des numéros de téléphone et d'informations sur les divisions
<b>NEW</b>	6.5	Facturation des coûts IT	Présentation des règles et planning de facturation des coûts IT

# 1

# Poste de travail

1. Matériel
2. Environnement de travail
  1. PC Management
  2. Mobile Management
3. Virtual Private Network
4. Système de messagerie
  1. Messagerie Outlook
  2. Sécurité de la messagerie
  3. Gestion des courriers indésirables
5. Liste de diffusion
6. Téléphonie Teams
7. Antivirus

# Matériel



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation  
Locale



Contrat  
VINCI

## 1.1 | Matériel

### ► RÈGLES



#### PC

Le catalogue matériel PC de VINCI Construction est issu du **catalogue de VINCI**. Au sein du catalogue de VINCI Construction, les **divisions/pays** sélectionnent les modèles qu'ils déploient dans leurs périmètres.

Pour les **PC**, les divisions et pays peuvent choisir de se fournir auprès d'un ou des deux fournisseurs HP et Lenovo, en fonction de leurs besoins, mais toujours des modèles du catalogue VINCI Construction.

En fonction des pays, les achats de PC peuvent se faire directement au **constructeur** ou via un **distributeur agréé** par le constructeur. La liste des distributeurs par pays et par constructeur est disponible auprès de l'équipe **Achats IT de VINCI Construction**.

Le prix des matériels PC inclut un **SAV premium** fourni par le constructeur, incluant une priorité sur la prise en compte des appels et sur le remplacement des pièces défectueuses via une ligne téléphonique dédiée et un code d'accès VINCI.

La durée d'utilisation recommandée des PC est de **5 ans avec la garantie standard**. Il peut y avoir des exceptions en fonction de leur utilisation et de stratégie des Divisions/Pays (par exemple, une utilisation intensive pour les calculs ou métiers spécifiques).

Les numéros de téléphone des SAV Lenovo et HP par pays et les codes d'accès sont disponibles auprès de l'équipe **Achats IT de VINCI Construction**.



#### Smartphones et tablettes

Le catalogue matériel smartphone/tablette de VINCI Construction est issu du **catalogue de VINCI**. Au sein du catalogue de VINCI Construction, les **divisions/pays** sélectionnent les modèles qu'ils déploient dans leurs périmètres.

Selon les pays, les pays/divisions peuvent choisir d'acquérir les smartphones avec l'abonnement mobile ou bien nus, via un distributeur de leur choix.

### ► RESSOURCES

Lien vers le catalogue du matériel PC et smartphones : [PC-Smartphones Catalogue FR.pdf](#) disponible dans le SharePoint VC IT Network.

## 1.2.1 | PC management

POSTE DE TRAVAIL

POSTE DE TRAVAIL

# PC management



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation  
IT Fees



Contrat

## 1.2.1 | PC management

### ► DESCRIPTION

Le poste de travail **UNITY** est basé sur la **solution Microsoft Intune**.

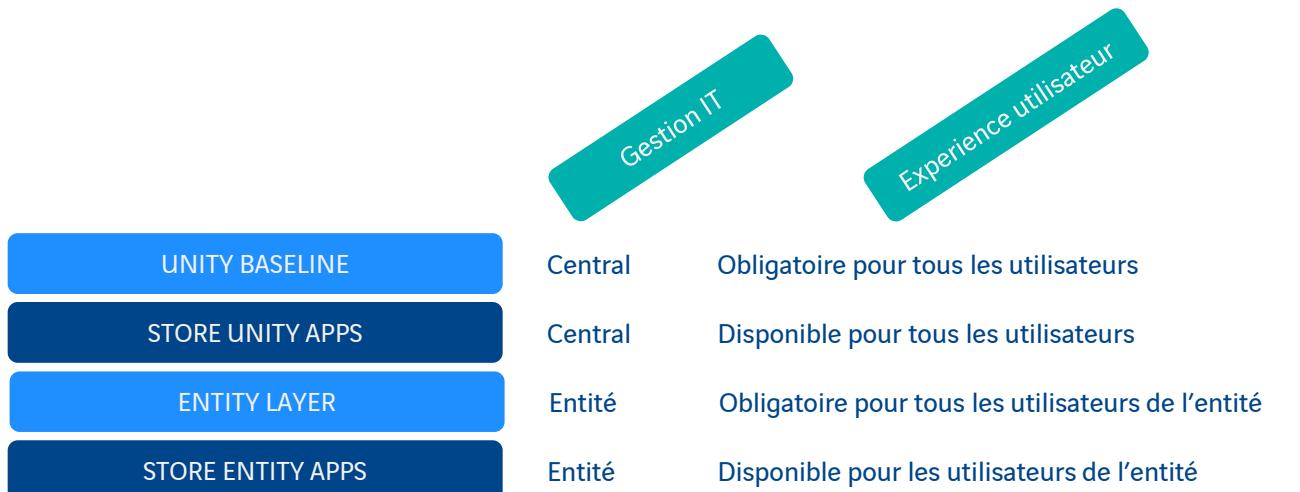
L'objectif est de **gérer l'ensemble des postes de travail du groupe dans un outil commun avec des règles communes** tout en permettant une personnalisation des Divisions.

Les postes de travail sont joints à **Microsoft Entra ID** commun au pôle pour permettre une authentification unique pour tous les collaborateurs VINCI Construction.

### ► RÈGLES

L'environnement applicatifs d'un PC dans Intune, s'organise en :

- Une **Baseline** (applications et paramètres) obligatoire et commune à tous les postes VINCI Construction.
- Un **Entity Layer** (applications et paramètres) obligatoire et commun à tous les postes d'une entité et défini par l'entité.
- Un **portail applicatif UNITY** qui permet aux utilisateurs d'installer des applications additionnelles. Pour les applications nécessitant une approbation (i.e.: licence) un workflow de validation sera disponible.



Le poste de travail UNITY peut être **préparé en dehors du réseau VINCI Construction**.

Il peut, également, à la demande, être préparé par le fabricant (HP/Lenovo/Autres) ou un tiers agréé et directement livré à l'utilisateur.

#### Paramètres par défaut :

##### Icônes du bureau

- ✓ Corbeille
- ✓ Portail UNITY
- ✓ mySupport
- ✓ OneTime Password (MFA)

##### Apps dans la barre d'outils et le menu Démarrer

- ✓ Chrome/Edge
- ✓ Teams
- ✓ Word, Excel, PowerPoint
- ✓ Capture d'écrans et croquis
- ✓ mySupport
- ✓ LogMeIn
- ✓ Les documents s'ouvrent directement dans l'application plutôt que dans Teams

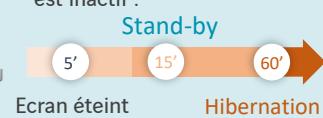


##### Fond d'écran géré par Bing

- ✓ Meilleure expérience utilisateur avec 1 nouveau fond tous les jours
- ✓ Aucun problème de droit à l'image

##### Gestion de la batterie

- ✓ 3 étapes existent, pour une gestion progressive de la batterie lorsque l'utilisateur est inactif :



Les entités et les utilisateurs pourront toujours modifier n'importe lequel de ces paramètres.

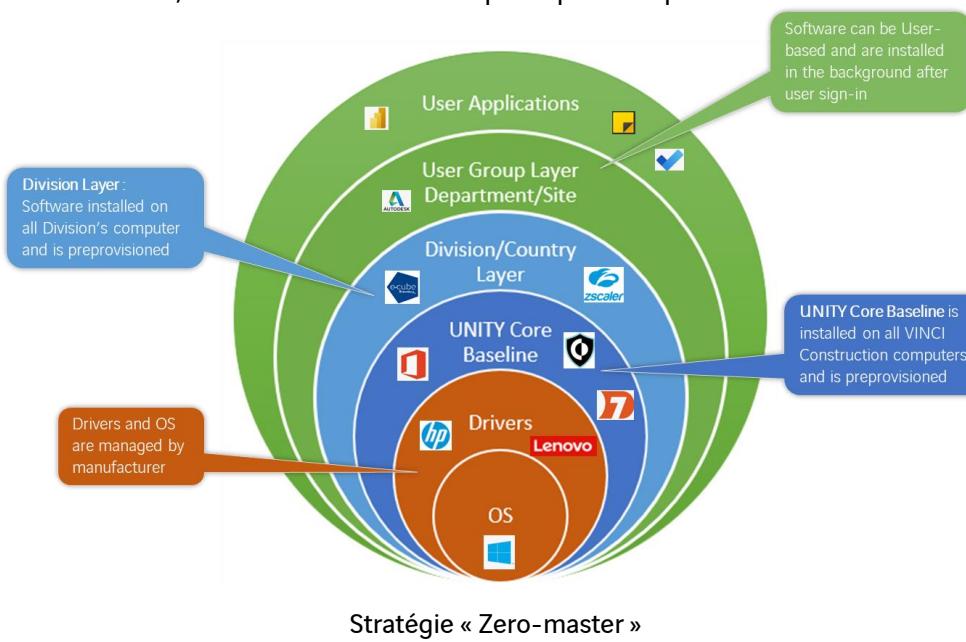
## 1.2.1 | PC management

### ► RÈGLES (suite) NEW

Les postes de travail intègrent automatiquement :

- Des standards de sécurité au niveau groupe comme les mises à jour automatiques Microsoft, le chiffrement des postes, l'authentification moderne (biométrie).
- La conformité aux règles de sécurité (CIS level 1) est évaluée en temps réel pour chaque poste et est utilisée pour autoriser ou bloquer l'accès aux ressources du groupe (posture zero-trust). Un poste de travail UNITY perdu ou volé pourra être bloqué à distance.
- Des bonnes pratiques d'optimisation de la batterie et de la consommation d'énergie (Green IT) : extinction automatique de l'écran et mise en veille en cas d'inactivité par exemple.

Le poste UNITY donne aussi plus d'autonomie et de service IT en libre-service à l'utilisateur : catalogue d'applications à la demande, réinitialisation du mot de passe par exemple.



Stratégie « Zero-master »

UNITY BASELINE	STORE UNITY
<p><b>Microsoft Apps</b> : Outlook, Teams OneDrive, Word Excel, PowerPoint, OneNote</p> <p><b>Navigateurs</b> : Edge, Chrome (navigateurs par défaut définis dans les ENTITY LAYERS)</p> <p><b>VPN</b> : Zscaler / Palo Alto</p> <p><b>Autres applications</b> : Cortex, Rapid7, LogMeIn, One Time Password (OTP), Polices VINCI</p>	<p>Si vous avez besoin de déployer une app; il est possible de la mettre à disposition par le store</p> 

Pour obtenir des droits d'administration sur un ordinateur UNITY, deux solutions sont disponibles :



Utilisateur

#### Admin By Request

Outil permettant à un utilisateur d'obtenir des droits d'administrateur sur son ordinateur.  
L'utilisation de l'outil doit être validée par le responsable et le RSSI de l'utilisateur



Admin

#### Compte LAPS

Outil permettant aux administrateurs d'obtenir le mot de passe de l'administrateur local des ordinateurs de son périmètre

## 1.2.1 | PC management

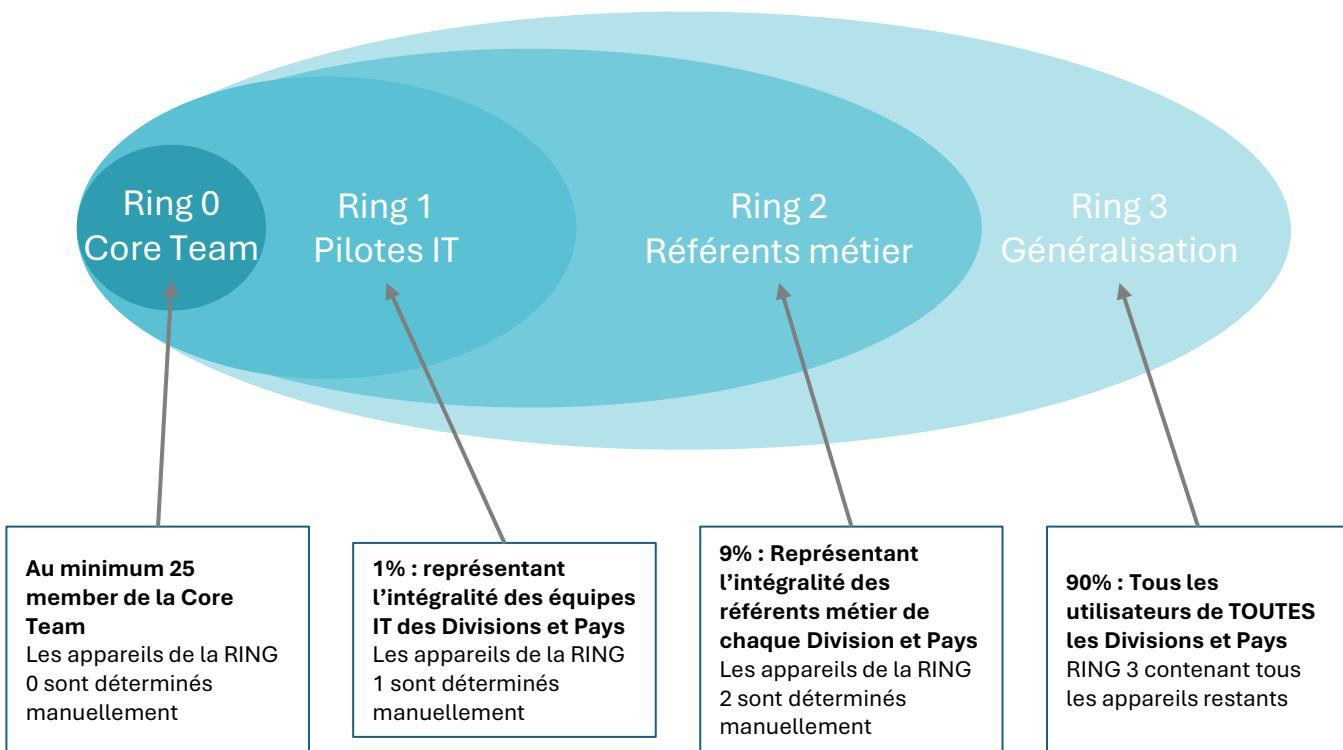
### ► RÈGLES (suite) NEW

Les postes de travail doivent **respecter les règles suivantes**:

- La **solution EDR** de VINCI Construction est installée, à jour et en cours d'exécution.
- La **solution VPN et SWG** de VINCI Construction est installée, à jour et en cours d'exécution.
- L'agent de la **solution de gestion des vulnérabilités** de VINCI Construction est installé, à jour et en cours d'exécution.
- Le **pare-feu** de l'appareil est activé.
- La **solution LAPS** du point de terminaison de VINCI Construction est appliquée.
- L'appareil est **crypté** avec BitLocker.
- L'appareil répond aux **règles de mise à jour** (incluses dans les Anneaux).
- La version du **système d'exploitation** de l'appareil est prise en charge et approuvée par la **cybersécurité**.

Les postes de travail sont **mis à jour suivant des "Ring"**. Qu'est-ce qu'une "Ring" ?

- Une Ring peut être **considérée comme un ensemble d'utilisateurs ou d'appareils**
- Une Ring est **planifiée selon une chronologie dépendante du produit**
- Une Ring permet **d'identifier d'éventuels problèmes et de pouvoir arrêter le déploiement avant d'impacter plus d'utilisateurs**



### ► RESSOURCES

Le suivi des indicateurs de gestions des postes de travail se fait au travers de [ce Dashboard](#).

## 1.2.2 | Mobile management

POSTE DE TRAVAIL

POSTE DE TRAVAIL

# Mobile management



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Mars 2024



Facturation  
IT Fees



Contrat

## 1.2.2 | Mobile management

### ► DESCRIPTION

Le nouvel appareil mobile **UNITY** basé sur la solution Microsoft Intune est proposé à l'ensemble des utilisateurs ne nos entités et divisions. L'objectif est de **gérer l'ensemble des smartphones et tablettes du groupe dans un outil commun avec des règles communes** tout en permettant une personnalisation locale.

L'ensemble des terminaux mobiles, **appartenant à la société ou équipements personnels**, accédant aux ressources du groupes sont concernés. L'objectif est de **sécuriser les données de VINCI Construction** sur l'ensemble des terminaux. Les terminaux respectent **les standards de sécurité communs** (chiffrement des données, verrouillage par code PIN, non « jailbreaké », mise à jour de sécurité appliquée) pour pouvoir accéder aux ressources de l'entreprise (posture zero-trust). En cas de **perte ou de vol du terminal**, l'accès du terminal est révoqué et les données d'entreprise peuvent être effacées.

### ► REGLES

Les appareils mobiles **sont gérés suivant les profils de configuration détaillés ci-dessous**.

Chaque division/entité a la possibilité de mettre en œuvre n'importe lequel de ces trois profils **indépendamment ou ensemble** en fonction des besoins utilisateurs. Les gammes supportées sont Android et IOS.

DEVICE MANAGEMENT & SECURITY	COPE Company Owned Personally Enable	COBO Company Owned Business Only	BYOD Bring Your Own Device				
	WORK PROFILE (PRO / PERSO SPLIT)	UNIQUE ENVIRONMENT	DEVICE ENROLLMENT & SUPERVISED	FULLY-MANAGED	SUPERVISED	MAM	MAM
Management of the device in Microsoft Intune	✓	✓	✓	✓	✓	✗	✗
Device registered in Azure AD	✓	✓	✓	✓	✓	✓	✓
Possibility to perform remote actions (Wipe, Retire, Push applications...)	✓	✓	✓	✓	✓	✗	✗
Security protections applied on compatible MAM applications	✓	✓	✓	✓	✓	✓	✓
Possibility to push policies to compatible applications	✓	✓	✓	✓	✓	✓	✓
Possibility to push policies to devices	✓	✓	✓	✓	✓	✗	✗
Personal and professional data treated in separate environments	✓	✗	✗	✗	✗	✗	✗

✓ Possible    ✗ Not possible

Profils disponibles - Vue IT

END-USERS FUNCTIONALITIES	COPE Company Owned Personally Enable	COBO Company Owned Business Only	BYOD Bring Your Own Device				
	WORK PROFILE (PRO / PERSO SPLIT)	UNIQUE ENVIRONMENT	DEVICE ENROLLMENT & SUPERVISED	FULLY-MANAGED	SUPERVISED	MAM	MAM
Access to pro and perso environments (Gmail / Outlook / Yahoo..)	✓	✓	✓	✓	✓	✓	✓
Access to the public Google Play Store or Apple AppStore	✓	✓	✓	✓	✓	✓	✓
Possibility to install all public applications (Instagram, WhatsApp..)	✓	✓	✓	✓	✓	✓	✓
Access to the enterprise store	✓	✓	✓	✓	✓	✗	✗
Possibility to install internal VC applications (E-Proc, E-HR ..)	✓	✓	✓	✓	✓	✗	✗
Unique environment for contact, video and photos management	✗	✓	✓	✓	✓	✓	✓

✓ Possible    ✗ Not possible    ⚡ Disabled by default – Can be modified by divisions

Profils disponibles – Vue utilisateur

## 1.2.2 | Mobile management

### ► RÈGLES (suite)

UNITY BASELINE	STORE UNITY
<b>Microsoft Apps</b> : Outlook, Teams OneDrive, Word Excel, PowerPoint, OneNote	Si vous avez besoin de déployer une apps; il est possible de la mettre à disposition par le store
<b>Autres applications</b> : MS Authenticator (MFA)	

### ► RESSOURCES

Le suivi des indicateurs de gesticions des smartphones se fait à travers un [Dashboard](#).

# Virtual Private Network



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Mars 2024



Facturation  
IT Fees



Contrat  
VINCI

## 1.3 | Virtual Private Network

### ► DESCRIPTION



Le service **VPN** « Virtual Private Network » permet de fournir un accès aux applications et services IT de VINCI Construction tout en assurant la **sécurité** des données de l'entreprise. Il est **obligatoire et actif en permanence** sur chaque poste utilisateur et se connecte de manière **transparente**.

Le VPN utilise le Single Sign-On (SSO) pour **ne pas avoir à ressaisir** son mot de passe.

**La solution groupe cible est Zscaler**, toutefois, tant que la migration n'est pas encore finie, certains périmètres utilisent d'autres solutions (Palo Alto/ Fortinet/ Autre).

Zscaler	Palo Alto (pôle version)	Local solutions
Cible	Inclus dans les IT Fees. Transition vers Zscaler en cours	Local IT Fees et management

### ► RÈGLES

Pour qu'il fonctionne, l'utilisateur doit **exister** dans les référentiels de l'entreprise et disposer d'un **compte**.

Il fait partie du socle des logiciels de **UNITY**.

L'**authentification** sur le VPN utilise des méthodes modernes et sécurisées (Microsoft Entra ID). En cas de blocage de certains sites web, il faut passer par le support local qui procédera au déblocage.

#### L'administration

Chaque division administrera son périmètre. Une équipe Core, composée d'administrateurs de la DSI Pôle et de différentes divisions, aura un rôle de Global Admin.

#### Les licences

Le principe de gestion des **licences est lié à l'utilisateur** pas à la machine. Ce qui veut dire qu'un utilisateur peut avoir sur son PC, sa tablette et son smartphone le client installé mais ne consommer qu'une seule licence.

# Messagerie Outlook



**Périmètre**  
Tout VINCI Construction



**Statut**  
Core



**Dernière mise à jour**  
Septembre 2024



**Facturation**  
Refacturation IT, selon grille tarifaire validée



**Contrat**  
VINCI

## 1.4.1 | Messagerie Outlook

### ► DESCRIPTION

La messagerie Outlook est disponible sur les postes de travail des utilisateurs avec le **client Outlook** ou via un **navigateur Internet** (Edge, Chrome) sur le [client web](#). Les licences sont attribuées aux utilisateurs via le **bundle** (Standard et Deskless), décrit [ici](#).

Le client Outlook permet de **gérer ses emails** et de **préparer ses envois**, même lorsque l'on est déconnecté. L'utilisateur peut également utiliser Outlook en application mobile sur son **smartphone** et/ou sa **tablette**.

### ► RÈGLES NEW

L'usage de la messagerie à des **fins personnelles n'est pas recommandé voire interdit selon les pays**. Veuillez-vous rapprocher de votre IT local pour plus d'informations.

Une **stratégie de rétention** définit les règles de gestion et de conservation des messages électroniques. Cette stratégie permet de conserver les données de la messagerie (**archivage légal**) en fonction des pays.

La boîte aux lettres possède un **quota de taille maximale** concernant tous les messages électroniques, les pièces jointes et les autres éléments. Lorsqu'une boîte aux lettres atteint son quota, un **avertissement** ou une alerte est envoyé(e) au propriétaire de la boîte aux lettres.

Licence	Espace de stockage	Quota***
<b>Standard (bundle)</b>	Boîte aux lettres utilisateur	100 Go
	Archive en ligne ( <i>en option, sans lien avec archivage légal</i> )	1,5 To, possibilité d'extension automatique limitée
<b>Deskless (bundle)</b>	Boîte aux lettres utilisateur	2 Go
-*	Boîte aux lettres partagée	50 Go**

\*Une **boîte aux lettres partagée** est une boîte aux lettres sans licence à laquelle plusieurs utilisateurs licenciés peuvent accéder pour lire et envoyer des messages électroniques.

\*\*L'**extension du quota de la boîte aux lettres partagée** est uniquement possible par l'ajout d'une nouvelle licence.

\*\*\*Quota: Il s'agit des quotas par défaut. Ces quotas peuvent être réduits sur demande.

#### Alertes de capacité

Si la taille de la boîte aux lettres **atteint ou dépasse la valeur spécifiée**:

- Exchange envoie un **message préalable d'avertissement** à l'utilisateur
- L'utilisateur **ne pourra plus envoyer** de nouveaux messages et verra un **message d'erreur**
- Tous les **messages reçus** seront **renvoyés** à l'expéditeur avec un **message d'erreur**

Quota boîte aux lettres	Alerte d'avertissement	Interdiction d'envoi	Interdiction d'envoi et réception
100 Go	98 Go	99 Go	100 Go
50 Go	48 Go	49 Go	50 Go
2 Go	1,96 Go	1,979 Go	2 Go

**Limites d'envoi et de taille des messages** (quel que soit le bundle):

Limite du nombre de destinataires	1 500 destinataires par jour
Nombre maximal de destinataires autorisés dans les champs À, Cc et Cci pour un seul message	500 destinataires
Limite de débit des messages	30 messages par minute
Restrictions sur la taille des messages - envoyés et reçus	50 Mo

NB : Pour la limite de débit maximal de destinataires et le nombre maximal de destinataires, un groupe de distribution stocké dans le carnet d'adresses partagé de l'organisation compte pour un destinataire.

## 1.4.1 | Messagerie Outlook

### ► RÈGLES (suite) NEW

#### Nom d'affichage - Gouvernance

Le "DisplayName" est le nom qui apparaît dans les courriels, les listes d'annuaires, les listes de contacts et lorsque l'utilisateur est mentionné ou interpellé dans les outils de collaboration et autres applications.

##### Configuration:

- Processus IAM (Identity and Access Management)
- Le service IT local peut mettre à jour le DisplayName dans l'Active Directory.

**Format (obligatoire avec le future COR/CPD):** NOMDEFAMILLE Prénom

# Sécurité de la messagerie



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Juin 2023



Facturation  
IT Fees



Contrat  
VINCI

## 4.1.2 | Sécurité de la messagerie

### ► DESCRIPTION

Pour prévenir les hameçonnages ou les usurpations d'identité, il existe trois **protocoles d'authentification** via le **DNS** (Domain System Name) :



Le protocole **SPF (Sender Policy Framework)** est une mesure de sécurité qui permet de **vérifier l'authenticité** des emails sortant en s'assurant que **l'adresse IP de l'expéditeur** est autorisée à envoyer des emails pour le domaine en question.



Le protocole **DKIM (DomainKeys Identified Mail)** est une méthode d'**authentification des emails** qui utilise une **signature numérique** pour vérifier que l'email sortant provient bien du domaine indiqué dans l'en-tête du message et que le contenu n'a **pas** été altéré pendant la transmission.



Le protocole **DMARC (Domain-based Message Authentication, Reporting, and Conformance)** est une méthode de **validation des emails** qui permet aux propriétaires de domaines de définir des **règles** pour indiquer aux serveurs de messagerie comment **traiter** les **messages entrants** qui ne passent **pas** les vérifications **SPF** et **DKIM**, et de fournir des informations de **rappor**t pour surveiller l'activité de messagerie pour leur domaine.

Toutes les applications envoyant des courriels avec nos domaines comme expéditeur et hébergées par un fournisseur **doivent être conformes** à l'exigence DMARC.

## 4.1.3 | Gestion des courriers indésirables

POSTE DE TRAVAIL

POSTE DE TRAVAIL

### Gestion des courriers indésirables



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation  
Fait partie de la licence M365



Contrat  
VINCI

## 4.1.3 | Gestion des courriers indésirables

### ► DESCRIPTION

Un mail est identifié **Spam** en fonction d'une **note pondérée** selon des critères modulaires et réglables par la DSI pôle : réputation de l'adresse IP du serveur d'envoi, émetteur (domaine de messagerie), contenu, adresse email source, quantité d'email, etc.

Les messages reçus peuvent être **catalogués** dans les Spam (alors que parfois, ils sont légitimes).

Cela peut s'expliquer par différentes raisons :

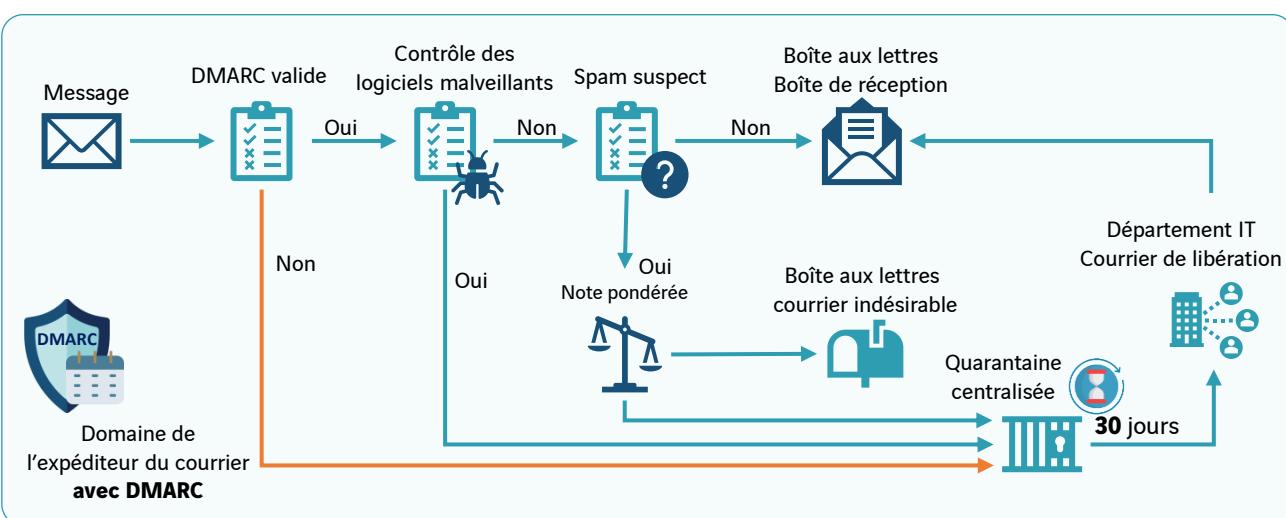
- Sur les **serveurs d'envoi** quand les enregistrements **SPF** (protocole Sender Policy Framework) et **DKIM** (protocole DomainKeys Identified Mail) sont **mal** ou **pas renseignés**.
- Sur le **poste client** avec l'**antispam** embarqué dans **Outlook** qui a ses propres règles.

### ► RÈGLES NEW

En cas d'email légitime mais considéré ou suspecté comme indésirable, les **étapes** suivantes sont à réaliser :

	E-mail en quarantaine que vous ne considérez pas comme Spam	E-mail reçu que vous considérez comme Spam
Support M365 VC	Il n'est pas possible de demander le <b>Whitelisting</b> (règle cybersécurité). Le support <b>analyse</b> le cas et fournit éventuellement les éléments nécessaires pour que <b>l'équipe IT de l'expéditeur</b> fasse les corrections.	Il n'est pas possible de demander le <b>Blacklisting</b> (règle cybersécurité). Le support <b>analyse</b> le cas et met en place les mesures de sécurité si nécessaire.
Équipe IT de l'expéditeur	Mise en <b>conformité</b> du <b>domaine</b> de l'émetteur (SPF/DKIM/DMARC)	

Toutes les applications envoyant des mails avec nos domaines comme expéditeur et hébergées par un fournisseur **doivent être conformes** à l'exigence DMARC. Pour toute question, un **ticket mySupport** doit être ouvert pour le service central **Microsoft 365**



# Liste de diffusion



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Mars 2024



Facturation  
IT Fees



Contrat

## 1.5 | Liste de diffusion

### ► DESCRIPTION

Il existe deux types de liste de diffusion : **statiques** et **dynamiques**.

- Les listes de diffusion **statiques** sont utilisées pour des périmètres de **petites tailles** (exemple : direction, groupe de travail).
- Les listes de diffusion **dynamiques** sont utilisées pour adresser des **périmètres importants**, en adressant tous les utilisateurs d'un périmètre donné (exemple : liste de diffusion pour une Délégation entière ou pour un pays entier). Ces listes sont établies sur les **propriétés AAD des utilisateurs** (pays, adresse, propriété du compte AD, etc.). Le **domaine de messagerie** ne peut **pas** être utilisé comme critère.

### ► RÈGLES

	Listes <b>statiques</b>	Listes <b>dynamiques</b>
<b>Qui peut créer les listes ?</b>	Central Support L1 et IT locaux avec droits d'administration O365 via une <b>demande de service</b> sur le portail mySupport	O365 L2 via une <b>demande de service</b> sur le portail mySupport
<b>Nomenclature (affichage)</b>	<b>_DL-&lt;DIV&gt;-&lt;DEL&gt;-&lt;LABEL&gt;</b>	<b>_DL-D-&lt;DIV&gt;-&lt;DEL&gt;-&lt;LABEL&gt;</b>
<b>Mise à jour des listes</b>	<ul style="list-style-type: none"><li>• <b>Par le propriétaire</b> de la liste depuis le <b>client Web Outlook</b></li><li>• Par les <b>équipes IT</b> via une <b>demande de service</b> sur le portail mySupport</li></ul>	<b>Automatique</b>

Toutes les listes de diffusion doivent être créées en mode **Cloud**.

Dans le cadre d'une liste de diffusion à **large échelle**, La DSI Pôle recommande de mettre en place un **modérateur** qui devra valider chaque usage de la liste de diffusion.

### ► RESSOURCES

Cliquez [ici](#) pour retrouver les **codes** de Divisions et Délégations à utiliser pour la nomenclature des listes.

Un [guide utilisateur](#) présentant les procédures à utiliser pour gérer les listes de diffusion est disponible sur le portail myHelp.

# Téléphonie Teams



**Périmètre**  
Tout VINCI Construction



**Statut**  
Modular



**Dernière mise à jour**  
Mars 2024



**Facturation**  
Refacturation IT, selon grille tarifaire validée



**Contrat**  
VINCI

## 1.6 | Téléphonie Teams

### ► DESCRIPTION

La **téléphonie Teams** permet à l'utilisateur d'utiliser Teams pour passer des **appels téléphoniques** vers des numéros fixes ou mobiles.

Voici quelques **fonctionnalités** disponibles avec la téléphonie Teams :



### ► RÈGLES

L'accès à la téléphonie Teams est **affecté sur demande**, en tant que licence complémentaire Office 365. Elle est destinée à **remplacer** les anciennes lignes fixes.

En complément de la **licence de téléphonie Teams (Phone System)** qui donne l'accès au service, il est nécessaire de souscrire à un **abonnement de téléphonie** pour disposer d'un numéro de téléphone, et ensuite pour pouvoir appeler des numéros et recevoir des appels.

Il existe pour cela **2 possibilités** :

	Calling Plan	Direct Routing
Souscription	Faire une demande de minutes de téléphonie comme les autres licences supplémentaires <b>Microsoft</b>	Souscrire un forfait de temps d'appels auprès d'un <b>opérateur de téléphonie</b> comme Orange
Avantages	<b>Facile et rapide</b> à déployer	Plus <b>économique</b> à l'utilisation
Points d'attention	<b>Coût à la minute</b> est plus élevé	Nécessite de <b>souscrire un contrat</b> auprès d'un <b>opérateur</b> et de passer par un <b>intégrateur</b> <b>Frais de setup</b> plus élevé

En fonction du type de **forfait** choisi et de l'**opérateur**, l'utilisateur peut accéder ou non aux **appels internationaux**. Dans tous les cas, les **appels reçus de l'extérieur** sont inclus dans les forfaits.

**Point d'attention** : un certain nombre de **prérequis** d'infrastructure sont nécessaires dans votre pays / entité avant de pouvoir offrir ce service aux utilisateurs. Pour être au fait de ces prérequis, contactez **le support local** via les équipes de Coordination.

## 1.7 | Antivirus

POSTE DE TRAVAIL

POSTE DE TRAVAIL

# Antivirus



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation  
Fees



Contrat  
VINCI

## 1.7 | Antivirus

### ► DESCRIPTION



#### Cortex XDR

L'antivirus de VINCI Construction est celui de Palo Alto Networks nommé Cortex XDR

Cet antivirus est une combinaison de **2 fonctions de sécurité principales:**

Nom	Description de la fonctionnalité
<b>Plateforme de protection des points finaux (EPP)</b>	La fonction EPP combine un <b>antivirus de nouvelle génération, un pare-feu personnel, le chiffrement, le contrôle des périphériques USB, l'évaluation des vulnérabilités</b> et bien d'autres choses encore, afin d'offrir une plateforme complète pour empêcher les logiciels malveillants de pénétrer dans les points d'extrémité.
<b>Détection et réponse des points finaux (EDR)</b>	La fonction EDR est principalement axée sur la <b>détection et l'investigation d'activités suspectes</b> .

La configuration et l'administration de cette solution se font directement dans le nuage fourni par Palo Alto.

### ► RÈGLES

L'agent est déployé sur tous les actifs : postes de travail, serveurs sur site et dans le nuage.

Tous les dispositifs de VINCI Construction partagent une protection commune, et **certaines exceptions locales peuvent être appliquées au niveau du pays.**

L'administration de cette solution suit un **modèle opérationnel fédéré**.

- Les administrateurs locaux peuvent gérer leurs propres actifs.
- Les administrateurs globaux peuvent gérer les règles et la configuration globales

Le cycle de vie de l'agent est géré de la même manière que les autres applications centrales d'UNITY.

## 2 | Infrastructure IT - Réseau

1. Réseaux disponibles
2. Wi-Fi

# Réseaux disponibles

NEW

RÉSEAU

RÉSEAU



Périmètre  
Tout VINCI Construction



Statut  
Local



Dernière mise à jour  
Septembre 2024



Facturation  
Local



Contrat  
Local

## 2.1 | Réseaux disponibles

### ► DESCRIPTION

Pour accéder aux applications de VINCI Construction ou du groupe VINCI, les **sites distants doivent être connectés au réseau privé**.

Il existe **différents types de connectivité** pour ces sites :

- Ligne **MPLS** des fournisseurs
- **Internet**:
  - Avec VPN au niveau des sites
  - Avec VPN au niveau des PC (connectés avec Zscaler)

Ces types de connectivité peuvent utiliser **plusieurs technologies de réseau**:



**DSL (Cuivre)**  
→ Une ancienne technologie sur le point de disparaître.



**Fibre (FTTH or FTTO)**  
→ La meilleure technologie pour la bande passante et la latence (pas déployée partout).



**Mobile (4G or 5G)**  
→ La 4G offre une bande passante limitée et la 5G n'est pas encore largement déployée.



**Satellite (GEO or LEO)**  
→ Les satellites LEO peuvent être déployés là où aucune autre option n'est disponible.

### Glossaire

Terme	Présentation
	<b>FTTH (Fiber To The Home)</b> Fibre optique partagée offrant une largeur de bande partagée entre les clients sur le même arbre optique
	<b>FTTO (Fiber To The Office)</b> Fournir une connexion dédiée avec une bande passante symétrique et garantie, adaptée aux grandes entreprises et aux utilisations critiques.
	<b>GEO (Geostationary Earth Orbit)</b> Cette offre de satellite est bonne mais a un temps de latence d'environ 600 ms.
	<b>LEO (Low Earth Orbit)</b> Fournir une largeur de bande comparable avec une latence nettement meilleure, de l'ordre de 30 ms

### ► RÈGLES

Quelques bonnes pratiques à suivre :

- Sécuriser la connectivité des utilisateurs en utilisant au moins l'un des types de connectivité suivants.
- Assurer la redondance, pour les sites critiques, en ayant deux lignes utilisant deux technologies différentes.
- Préférer l'utilisation d'une solution SD-WAN plutôt que des solutions MPLS.
- Pour tous les appareils de l'entreprise, Zscaler est obligatoire.

# Wi-Fi

NEW

RÉSEAU

RÉSEAU



Périmètre  
Tout VINCI Construction



Statut  
Local



Dernière mise à jour  
Septembre 2024



Facturation  
Local



Contrat  
Local

## 2.2 | Wi-Fi

RÉSEAU

RÉSEAU

### ► DESCRIPTION



Le Wi-Fi est un réseau local sans fil qui permet aux utilisateurs d'accéder à des applications. Contrairement aux réseaux mobiles (4G ou 5G), le Wi-Fi est lié à un site spécifique.



Il existe 3 types de réseaux Wi-Fi, appelés SSID (Service Set Identifiers) :

- **SSID internet** → Permet l'accès au réseau internet
- **SSID Guest** → Accès temporaire à internet à la demande pour les utilisateurs externes de VINCI Construction
- **SSID uniVINCI** → Accès automatique à Internet pour tous les utilisateurs de VINCI.

Pour fournir le Wi-Fi sur un site, vous devez acheter une infrastructure avec des points d'accès.

### ► RÈGLES

Actuellement, le Wi-Fi est une **solution locale**, c'est-à-dire qu'il n'y a pas de contrat global ou de solution fournie par VINCI Construction Central IT.

Les règles peuvent varier d'un pays à l'autre, en fonction des **contraintes juridiques locales**.

*Pour exemple : En France, les journaux de connexion des visiteurs doivent être conservés pendant un an.*

Pour le **SSID interne**, il est essentiel de s'assurer que seuls les appareils autorisés peuvent accéder à ce réseau. Une politique de conformité doit être mise en place pour authentifier les appareils (certificat, inscription au domaine, ...).

Pour le **SSID uniVINCI**, l'authentification est basée sur les utilisateurs et/ou les machines.

Ce SSID peut identifier le pôle d'affiliation d'un utilisateur ou d'un appareil et le valider en conséquence.



Il est recommandé de déployer le SSID uniVINCI partout afin de s'assurer que tous les utilisateurs de VINCI ont accès à l'Internet Wi-Fi dans n'importe quel lieu de VINCI.

# 3 | Infrastructure IT - Serveurs & Cloud

1. Cloud privé
2. Cloud public
3. Archivage
4. Scan de vulnérabilité

## Cloud Privé (NGDT)



Périmètre  
Tout VINCI Construction



Statut  
Modular



Dernière mise à jour  
Mars 2024



Facturation  
Refacturation IT



Contrat  
VINCI Construction

## 3.1 | Cloud privé

### ► DESCRIPTION

Le Cloud privé (**Next Gen Datacenter - NGDT**) est un service de fourniture d'environnements virtualisés supportant tout le cycle de production d'applications avec :

- Un **hébergement de vos données en France**.
- La **gestion des machines virtuelles (VMs)** via un portail self-service.
- Gérer l'**obsolescence** des équipements et des logiciels en mettant en place une stratégie proactive pour éviter les interruptions de service et les coûts excessifs liés aux équipements obsolètes.

L'accès à un **portail** permet de suivre l'**usage** et la **consommation** des ressources allouées.



Cloud **souverain** hébergé en France



Infrastructures redondées entre **deux** datacenters



Sauvegardes **quotidiennes**, **hebdomadaires** et **mensuelles**



Haute disponibilité **24/7**

### ► RÈGLES

- La capacité de la plateforme étant dimensionnée par rapport au besoin actuel, toute demande significative doit être **anticipée**.
- La facturation est **annuelle** sur une base de consommation **quotidienne**.
- L'acquisition des licences logicielles et l'accès au service sera à **confirmer** avec la DSI Pôle.
- **Systèmes d'exploitation** et **dimensionnement de la VM** disponibles selon catalogue de services.  
Plage de support 8h30-18h hors jours non ouvrés (5j/7).

Gestion par la Division	Mise à disposition de VM (IaaS)	IaaS et système d'exploitation (IaaS+)	IaaS+ et composants techniques (PaaS)
	Applications	Applications	Applications
	Données	Données	Données
	SGBD	SGBD	SGBD
	Middleware	Middleware	Middleware
	Système d'exploitation	Système d'exploitation	Système d'exploitation
	Virtualisation Hypervision	Virtualisation Hypervision	Virtualisation Hypervision
	Serveurs physiques	Serveurs physiques	Serveurs physiques
	Stockage physique	Stockage physique	Stockage physique
	Réseau	Réseau	Réseau
	Hébergement physique	Hébergement physique	Hébergement physique

### ► RESSOURCES

- Le **calcul des coûts** se fait via la calculette NGDT. Ils sont réévalués tous les ans.
- Les indicateurs de monitoring sont :

Nom	Description	Périodicité	Seuil
% disponibilité du service	= durée d'indisponibilité du service (hors plage de maintenance) / durée d'ouverture du service	Annuelle	99,5 % = 216 min/mois
% incidents hors SLA	= nombre d'incidents dont la durée de traitement a excédé le SLA / nombre total d'incidents de la période (SLA = 8h pour P1, 24h pour les autres incidents)	Annuelle	10 %

## Cloud Public



Périmètre  
Tout VINCI Construction



Statut  
Modular



Dernière mise à jour  
Mars 2024



Facturation  
Refacturation IT



Contrat  
VINCI Construction

## 3.2 | Cloud public

### ► DESCRIPTION

Le Cloud public est la fourniture de zones hébergements avec :

- Une sélection des services hébergés sur **Azure** et/ou **AWS** intégrés aux politiques de gouvernance, d'architecture et sécurité de la DSi Pôle (IaaS, PaaS, Saas, XaaS, API, ...)
- Une scalabilité verticale ou horizontale en fonction de l'architecture applicative.

L'accès à un **portail** permet de suivre l'**usage** et la **consommation** des ressources allouées en temps réel.



Cloud mondial



Infrastructures managées



Sauvegardes calibrées



Disponibilités adaptées

La gamme de services **Azure** et **AWS** intégrée par la DSi Pôle couvre actuellement différents domaines :



**Calcul**,  
des machines virtuelles,  
des fonctions serverless et  
des services d'équilibrage  
de charge,  
permettant d'exécuter des  
applications et de gérer des  
ressources de manière  
flexible et évolutive.



**Stockage et archivage**,  
d'objets, de fichiers, de  
blocs, d'archives,  
permettant de gérer les  
données de manière  
sécurisée et hautement  
disponible.



**Bases de données**,  
tels que les bases  
relationnelles, NoSQL,  
bases de données en  
mémoire, et des services  
de gestion de données  
(type Data Lake et Data  
Factory).



**Mise en réseau**,  
tels que la mise en réseau  
virtuel, l'équilibrage de  
charge et des services de  
passerelles.



**Sécurité et conformité**,  
pour protéger les données,  
les identités et les  
ressources contre les  
menaces et garantir la  
conformité réglementaire.

En parallèle, sur la base d'Azure DevOps, la DSi Pôle a développé et met à disposition une gamme de compétences et d'outils pour le support au **développement d'applications** :

- L'infrastructure as code (**IaC**) permettant de mettre à disposition de façon automatisée (via Terraform, Packer):



Une **landing zone**  
sécurisée aux standards  
de la DSi Pôle



Des environnements  
configurés et segmentés  
**(DEV, UAT, PPD, PRD)**



La gestion des **identités** (RBAC)  
et la création de **comptes** dans  
Microsoft Entra ID



La gestion des **secrets**  
avec Azure Key Vault

- Une gestion **d'artifact** et des **templates** de déploiement (Continuous Deployment)
- Des **bacs à sable** pour tester de nouvelles solutions en toute sécurité, non connectés au SI de la DSi Pôle

Ce catalogue est en évolution constante avec l'intégration de nouveaux composants qui devraient amener à un template de chaîne **CI/CD** complète (Azure DevOps, Ansible, Terraform) et conforme aux exigences de la DSi Pôle.

### ► RÈGLES

- La capacité de la plateforme est **illimitée** et peut s'adapter en temps réel au besoin.
- Le **catalogue de service** proposé est une sélection des services hébergés sur **Azure** et/ou **AWS** intégrés aux politiques de gouvernance, d'architecture et sécurité de la DSi Pôle.
- Une plateforme **FinOps** permet de suivre la facturation **mensuelle** sur une base de consommation **horaire**.
- L'acquisition des licences logicielles et l'accès au service sera **à confirmer** avec la DSi Pôle.
- **L'accès au service se fait via une landing/availability zone construite et gérée par la DSi Pôle. La délégation de droits est traitée au cas par cas.** Une policy est en cours de rédaction.
- **Le support aux opérations** est disponible de 5j/7 8h30-18h (heure Paris).
- L'utilisation d'Azure DevOps n'est pas obligatoire mais permet de bénéficier des automatismes développés dans les environnements Azure et AWS.

### ► RESSOURCES

- Le **calcul du coût** se fait via le calculateur du cloud provider **Azure** ou **AWS**.

Nom	Description	Périodicité	Seuil
% disponibilité du service	= durée d'indisponibilité du service (hors plage de maintenance) / durée d'ouverture du service	Annuelle	99,5 % = 216 min/mois
% incidents hors SLA	= nombre d'incidents dont la durée de traitement a excédé le SLA / nombre total d'incidents de la période (SLA = 8h pour P1, 24h pour les autres incidents)	Annuelle	10 %

# Archivage



Périmètre  
Tout VINCI Construction



Statut  
Modular



Dernière mise à jour  
Septembre 2024



Facturation  
A définir



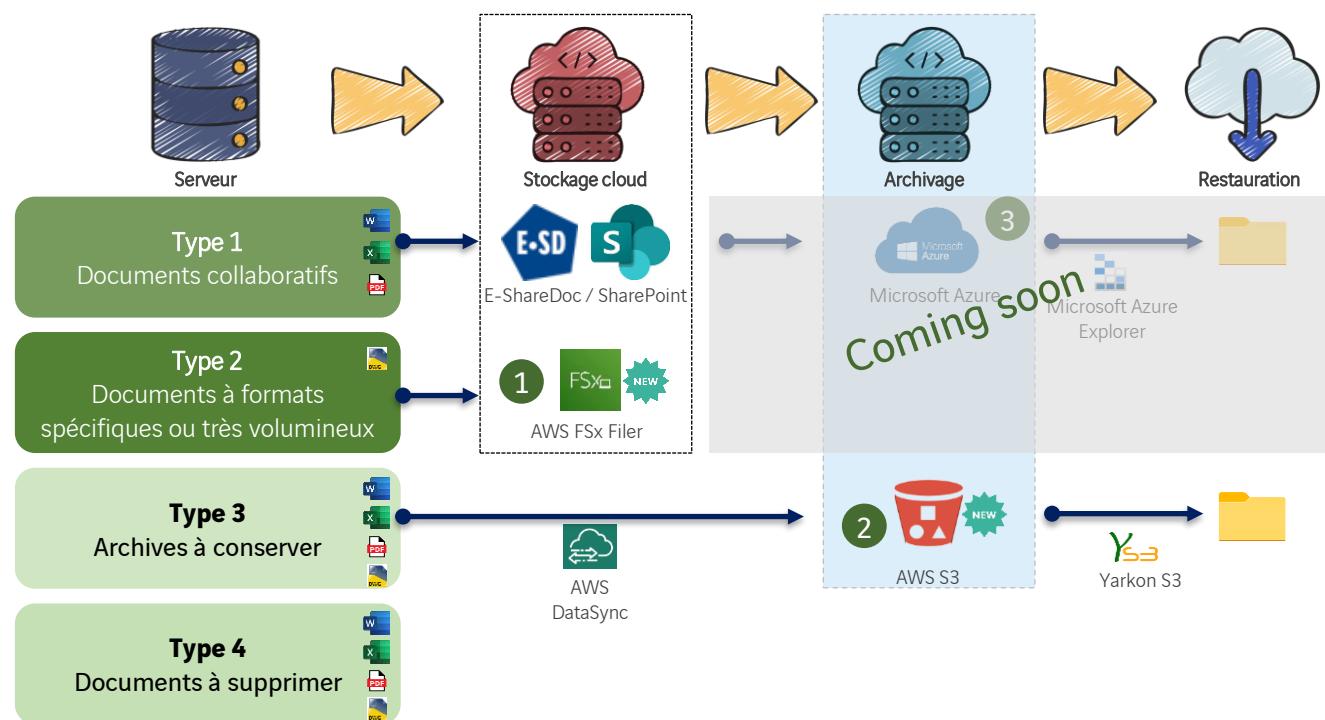
Contrat

-

## 3.3 | Archivage

### ► DESCRIPTION NEW

Voici les services disponibles pour stocker et archiver les documents des serveurs physiques.



### ► RÈGLES

Cas d'usage	1 Stockage documents spécifiques ou volumineux (>1Go) en alternative à SharePoint	2 Archivage des documents depuis un serveur d'Agence	3 Archivage des SharePoint (y compris E-ShareDoc)
Outil	FSx for Windows 	S3 Instant Retrieval 	Microsoft Azure 
Quand l'utiliser ?	Si problématique d'exploitation via SharePoint pour des documents à formats spécifiques ou volumineux	Avant de décommissionner un serveur, pour stocker les documents « à conserver » mais inutilisés	Dans le cadre du cycle de vie des documents, pour stocker les documents « à conserver » mais inutilisés
Qui l'utilise ?	Bureaux d'Etudes, Géomètres, Chefs d'Agences, Chefs de secteur	Chef d'Agence, RFA, Correspondant Informatique, Chefs de secteur ...	Les personnes habilitées dont les propriétaires
Comment l'utiliser ? (myHelp)	Ajouté ( <a href="#">lien myHelp FSx</a> )	A mettre à jour ( <a href="#">lien myHelp AWS S3</a> )	
Comment le mettre en place ?	- Mise en place technique d'un espace de stockage (DSI Pole) - Définir les droits pour les utilisateurs habilités (IT Local)	- Mise en place technique d'un espace de stockage (DSI Pole) - Définir les droits pour les utilisateurs habilités (IT Local) - Migration documentaire (DSI Pole)	
Capacité stockage	- Délégation : 64To - Agence : 2To extensibles	- Non définie	- Non définie

## Scan de vulnérabilité



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Mars 2024



Facturation  
IT Fees



Contrat  
VINCI Construction

## 3.4 | Scan de vulnérabilité

### ► DESCRIPTION

**Rapid7** est la solution du groupe VINCI Construction pour **scanner son parc informatique** et **déetecter des vulnérabilités** potentielles.

Rapid7 permet d'avoir une bonne **visibilité de l'ensemble du parc informatique** connecté au réseau de VINCI Construction (PC, serveur, imprimante, équipement réseau...) et remonte ainsi pour chaque équipement un **inventaire des logiciels installés**.

Rapid7 détecte les vulnérabilités sur les applications et les systèmes d'exploitation, en s'appuyant sur les bases de données mondiales. Il **n'assure pas la remédiation** des vulnérabilités.

### ► RÈGLES

Rapid7 scanne le parc informatique en utilisant **2 méthodes** :

Comment	Fréquence de scan	Cible
Avec un agent	En temps réel	PC et Serveur
Via un scan réseau	1 fois par semaine	Tout type d'équipement

**L'agent** Rapid7 fait partie du socle **UNITY**.

Le serveur de scan est indispensable pour identifier des équipements informatiques qui ne sont pas des PC ou des serveurs, et qui sont connectés au réseau de VINCI Construction.

#### Les licences

Les licences sont attribuées pour **chaque équipement** qui a été scanné à la recherche de **vulnérabilité**.

# 4

# Identité & Référentiel

1. Licences utilisateurs
2. Licences à la carte
3. Comptes standards et comptes à priviléges
4. Authentification forte
5. Accès conditionnels
6. Référentiels d'architecture

# Licences utilisateurs (bundles)



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation  
Refacturation IT, selon grille tarifaire validée



Contrat  
VINCI

## 4.1 | Licences utilisateurs (bundles)

### ► DESCRIPTION NEW

Les licences Microsoft 365 donnent accès à des services en fonction des **besoins** des utilisateurs.

3 types de profils sont disponibles :

#### Bundle Standard (E3)



Utilisateur PC

#### Bundle Deskless (F1+F3)



Utilisateur mobile avec boîte aux lettres

#### Bundle Mailboxless (F1)



Utilisateur mobile sans boîte aux lettres

L'attribution des licences Microsoft 365 est **déléguee** par des groupes de sécurité synchronisés :

Bundle	Groupe
Standard (bundle)	GRP-<DIV>-<DEL>-LIC-STANDARD
Deskless (bundle)	GRP-<DIV>-<DEL>-LIC-DESKLESS
Mailboxless (bundle)	GRP-<DIV>-<DEL>-LIC-MAILBOXLESS

Les groupes de délégation sont déjà créés dans **l'Active Directory** et sont gérés par les **IT locaux**.

**L'attribution d'une licence (bundle)** à un utilisateur, peut se faire de plusieurs manières:

- Ajouter le compte de l'utilisateur **manuellement** dans le groupe de licences.
- Ajouter le compte de l'utilisateur **automatiquement** (via script)
- Via création d'un **ticket ITSM** (process interne division/délégation)

Si la **licence actuelle** n'inclut pas les fonctionnalités ou les applications dont l'utilisateur a besoin, il peut être nécessaire de **mettre à niveau** la licence.

Il est possible de **changer** de bundle : pour cela, l'**IT local** transfère l'utilisateur dans le **groupe de licence** pour lui assigner le nouveau bundle.

#### Exemple : Passage d'une licence Deskless à Standard

➔ L'IT local supprime le compte utilisateur du groupe GRP-VIC-MLIC-DESKLESS-<Code Division> et l'ajoute dans le groupe GRP-VIC-MLIC-STANDARD-<Code Division>.

#### Dans le cas d'un passage de licence de Standard à Mailboxless :

➔ L'utilisateur perd l'accès à sa boîte aux lettres.

#### Dans le cas d'un passage de licence de Standard à Deskless :

➔ L'utilisateur peut rencontrer des problèmes d'envoi et de réception de mails si l'usage de sa boîte aux lettres a dépassé les 2 Go (limite de l'offre Deskless).

Au-delà de ces 3 bundles, il existe aussi une offre de boîte aux lettres partagées: **Shared Mailbox**. Disponible à la demande via l'ITSM. Elle est réservée aux usages d'équipes.

## 4.1 | Licences utilisateurs (bundles)

### ► RÈGLES NEW

		Standard (E3)	Deskless (F1+F3)	Mailboxless (F1)	Shared Mailbox
Caractéristiques M365	Office Online (via navigateur)	Modifier les docs Office 365	✓	✓	✓
	Defender for Office 365 Plan 1	A préciser	✓	✓	✓
	Audio Conf Dial In	A préciser	✓	✗	✗
	SharePoint Online	Accès aux sites collaboratifs (en ligne)	✓	✓	✓
	MFA	Authentification forte	✓	✓	✓
	OneDrive for Business		2 To	2 Go	2 Go
	Viva Engage (ex-Yammer)		✓	✓	✓
	Teams		✓	✓	✓
Fonctionnalités Boîte aux lettres	Licences à la carte (facturées) : PowerBI, Project, Visio		✓	✓	✗
	Quota de la boîte aux lettres*	Taille limite de la boîte aux lettres	100 Go	2 Go	✗
	Délégation aux autres boîtes aux lettres		✓	✓	✗
	Quota d'archives en ligne	Déplacement des emails vers l'archivage Cloud "Conservation légale" gardant une trace des boîtes aux lettres supprimées	100 Go	✗	✗
	Archivage légal	Notifications lorsque la boîte aux lettres est proche ou au maximum de sa capacité	✓	✗	✗
	Alertes de capacité		✓	✓	✗
	Rétention de la boîte aux lettres (sur demande)	Restaurer la boîte aux lettres supprimée < X années après sa suppression	✓	✗	✗
	E-mails déplacés vers les dossiers "Éléments supprimés"		✓	✓	✗

\***Office sur le web** : pour les licences M365 F1, les applications sont en lecture seule.

\***Boîte aux lettres partagée** : par défaut, pas de licence nécessaire, sauf si le quota est atteint.

\***Quota de la boîte aux lettres** : Il s'agit des quotas par défaut. Ces quotas peuvent être réduits sur demande.

### Stockage individuel

OneDrive facilite la mobilité, il est accessible en ligne avec un **navigateur web** et via une **application mobile** sur smartphone ou tablette.

Un client permet de configurer l'accès en **mode déconnecté** (pour travailler sans avoir accès à Internet).

Comme tous les outils professionnels, le OneDrive contient des **données de travail**.

Il s'agit d'un outil à **usage individuel**, dont les fichiers ne doivent être partagés que ponctuellement.

Après le **départ** d'un **collaborateur**, son OneDrive reste en **rétention** pendant **12 ans**.

Si le manager est renseigné dans Microsoft Entra ID, alors il reçoit un lien permettant d'accéder au compte OneDrive du collaborateur. Le lien reste valide pour **30 jours**.

# Licences à la carte



Périmètre  
Tout VINCI Construction



Statut  
Modular



Dernière mise à jour  
Septembre 2024



Facturation  
Refacturation IT, selon grille tarifaire validée



Contrat  
VINCI

## 4.2 | Licences supplémentaires à la carte

### ► DESCRIPTION NEW

Pour permettre aux utilisateurs d'accéder à un service ou une fonctionnalité d'un service Office 365 **à la carte** (Visio Plan 2, Project Plan 3, Power BI Pro, etc.), il faut leur assigner des licences. Pour des raisons de facilité de gestion, ces licences sont attribuées aux utilisateurs en fonction de leur **groupe d'appartenance**.

La DSI Pôle propose des **licences payantes supplémentaires** sous différentes catégories. Ci-dessous un **exemple** de ces licences :

		Licences
<b>Teams</b> 	Licences Téléphonie Teams	<ul style="list-style-type: none"><li>▪ Teams Phone Standard</li><li>▪ Teams Phone Resource Account</li></ul>
	Licences supplémentaires du système téléphonique	<ul style="list-style-type: none"><li>▪ Teams Domestic and International Calling Plan</li><li>▪ Teams Domestic Calling Plan</li><li>▪ Teams Domestic Calling Plan 120 minutes</li><li>▪ Teams Domestic Calling Plan 240 minutes</li></ul>
<b>Office 365</b> 	Autres	<ul style="list-style-type: none"><li>▪ Teams Rooms Standard</li><li>▪ Communication Credit</li></ul>
	Licences SharePoint Online	<ul style="list-style-type: none"><li>▪ SharePoint Syntex</li><li>▪ Dynamics 365 Remote Assist</li><li>▪ Dynamics 365 Sales Enterprise</li></ul>
	Autres	<ul style="list-style-type: none"><li>▪ Power Apps per user plan</li><li>▪ Power Automate per user plan</li><li>▪ Power BI Pro</li><li>▪ Visio Plan 2</li><li>▪ Project Plan 3</li><li>▪ Project Plan 5</li></ul>

L'attribution des licences supplémentaires à la carte est déléguée par des **groupes de sécurité synchronisés**. Ci-dessous un **exemple** de ces groupes :

Licence	Groupe
Project Plan 3	GRP-VIC-MLIC-PROJECTPLAN3-<Code Division>
Project Plan 5	GRP-VIC-MLIC-PROJECTPLAN5-<Code Division>
SharePoint Syntex	GRP-VIC-MLIC-SPOSYNTEX-<Code Division>
Visio Plan 2	GRP-VIC-MLIC-VISIOPLAN2-<Code Division>
Communication Credit	GRP-VIC-MLIC-COMCREDIT-<Code Division>
Power BI PRO	GRP-VIC-MLIC-POWERBIPRO-<Code Division>

Les groupes de délégation sont déjà créés dans **l'Active Directory** et sont gérés par les **IT locaux**. Ces groupes seront prochainement transférés dans Microsoft Entra ID.

Pour **attribuer une licence supplémentaire** à un utilisateur, l'**IT local** peut ajouter le compte de l'utilisateur dans le **groupe de licences** de la Division/Délégation.

Pour modifier « le plan » d'une licence, l'**IT local** doit transférer le compte de l'utilisateur dans le nouveau groupe correspondant.

#### Exemple : Upgrade d'une licence Project Plan 3 vers Project Plan 5

→ L'IT local supprime le compte utilisateur du groupe  
l'ajoute dans

# Comptes standards et comptes à privilèges



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation  
IT Fees



Contrat  
VINCI Construction

## 4.3 | Comptes standards et comptes à privilèges

### ► DESCRIPTION

Un compte informatique permet une utilisation **sécurisée, personnalisée** et **contrôlée** des ressources numériques.

Il est généralement composé d'un **nom d'utilisateur** et d'un **mot de passe** pour assurer la sécurité et l'authentification.

Les comptes sont souvent associés à des profils **utilisateurs**, définissant les **droits** et **restrictions** de chaque individu. Les **administrateurs** système (ou responsables d'applications) peuvent gérer ces comptes en **ajoutant, modifiant ou supprimant** des utilisateurs et leurs accès.

### ► RÈGLES NEW

**Gestion des accès** : Les accès aux systèmes et aux données ne sont accordés uniquement qu'aux personnes qui en ont besoin pour effectuer leur travail. Toutes demandes relatives aux accès sont tracées via un ticket **mySupport**.

**Utilisation du Single Sign-On (SSO)** : si l'application le permet, l'authentification à l'application doit se faire en **SSO** via EID (OIDC / SAML 2.0).

**Limitation des privilèges** : Les comptes **standards** ne fournissent pas de privilèges et permettent l'usage quotidien des outils informatiques. Pour les utilisateurs avec des **rôles d'administration**, la règle est de ne pas fournir plus de privilèges que nécessaire pour effectuer leur travail (règle du moindre privilège).

**Utilisation de mots de passe forts :**

- **Comptes normalisés** : la politique de sécurité des systèmes d'information (PSSI) définit les règles spécifiques de l'entreprise en matière de mots de passe. Retrouvez la PSSI sur le [portail cybersecurité de VINCI](#).
- **Comptes à privilèges** : voir le document [règles d'authentification pour les comptes à privilèges](#).

**Désactivation et suppression** des comptes privilégiés non utilisés (pour ADT, ADA, ADS, ADC, SEC, ADM et WS) :

Désactivation après **60** jours d'inactivité



« Soft delete » après **120** jours d'inactivité



« Hard delete » après **150** jours d'inactivité

## 4.3 | Comptes standards et comptes à privilèges

### ► RÈGLES (Suite) NEW

Ci-dessous le tableau des différents comptes à privilèges :

Catégorie des comptes	Description	Type	Exemple	
Comptes Tier0	<b>ADF</b>	Administrateur de l'entreprise AD	H_ADF_ADDS_XXXX	
	<b>ADD</b>	Administrateur d'un domaine	H_ADD_ADDS_XXXX	
	<b>Z*</b>	Administrateur d'un domaine	ZLASTNAME	
	<b>OPS</b>	Opérateur du Tier0 (pour se connecter sur les PAW)	On Premise	H_OPS_ADDS_XXXX
	<b>ADC</b>	Administrateur des services Active Directory (GPO, sites AD, PAW) Administrateur des services centraux Tier0 (Check_MK, SEPM, Vmware, ADFS, CERT, WSUS MDT...)	H_ADC_CERT_XXXX	
<APPLICATION>_<ENV><DATE><X>		Compte de service	Hybrid / On Premise	
Comptes serveurs	<b>ADC</b>	Administrateur central des infrastructures communes VC-IC (Maestro, Exchange, SI Compta, O365...)	adc_firstname.lastname	
	<b>ADM*</b>	Administration centrale des serveurs applicatives et des objets Active Directory	adm-lastname	
	<b>ADS</b>	Administrateur dans les divisions (Matis, LIP, Hermes...)	ads_firstname.lastname	
	<b>SEC</b>	Compte administratif pour les appliances Fortigate	sec-lastname	
<APPLICATION>_<ENV><DATE><X>		Compte de service	ORGN_PXXXXXXXXX	
Comptes Poste de travail	Administrateur des périphériques des utilisateurs (ordinateurs, imprimantes et téléphones portables)			
	<b>ADS</b>	Opérateur de comptes Active Directory non-administrateurs	Hybrid / On Premise	ads_firstname.lastname
	Administrateur du groupe de sécurité Active Directory			
Comptes Cloud only AAD	<b>ADL</b>	Administrateur local d'une machine Vpod	adl_firstname.lastname	
	<b>WS*</b>	Administrateur local des ordinateurs de la division ou d'un ordinateur individuel	On Premise	ws-flastname
	<b>ADW</b>	Compte à privilège ADW (Amazon)	adw_firstname.lastname@vinci-construction.com	
	<b>ADO</b>	Compte à privilège HLD ADW (Amazon)	ado_firstname.lastname@vinci-construction.com	
	<b>ADA</b>	Administrateur de services Azure	ada_firstname.lastname@vinci-construction.com	
<b>ADT</b>		Administrateur du tenant O365 et de Microsoft Entra ID (Global Admin O365)	adt_firstname.lastname@vinci-construction.com	

\* : ex-Eurovia France

# Authentification forte (MFA)



Périmètre  
VINCI Construction



Statut  
Core



Dernière mise à jour  
Juin 2023



Facturation  
Inclus dans les licences utilisateurs



Contrat  
VINCI

## 4.4 | Authentification forte (MFA)

### ► DESCRIPTION

L'**authentification forte** (MFA pour Multi-Facteurs Authentification) permet de s'identifier de manière sécurisée à vos outils professionnels grâce à une méthode de sécurité renforcée. Une **notification d'approbation** ou un **code aléatoire** apparaît sur smartphone, en plus du mot de passe habituel. Cette méthode permet de limiter les risques d'usurpation d'identité et de vol de données sensibles.

### ► RÈGLES

Tous les **90 jours**, lorsque vous souhaitez vous connecter à **Office 365**, une demande d'authentification via le **MFA** vous sera demandée.

Chez VINCI Construction, l'application **Microsoft Authenticator** est la méthode préconisée. Il est aussi **possible** d'utiliser l'application PC OneTime Password ou le SMS comme méthode de connexion en cas d'indisponibilité de la première méthode préconisée.

**Par défaut, tous** les comptes sur **Microsoft Entra ID** ont le MFA **activé**. Seuls les **comptes de services** sont exemptés de MFA.

Lors d'une notification Microsoft Authenticator, la **zone géographique** de connexion est indiquée à titre indicatif (basée sur les informations de votre opérateur téléphonique) et peut être imprécise lorsque vous êtes connecté au **VPN**. Elle permet de vérifier d'où provient la demande, afin d'**éviter une usurpation d'identité** réalisée à partir d'une autre zone géographique.

Pour la gestion des exclusions MFA :

- Les comptes de services sont placés dans des **groupes Microsoft Entra ID** qui permettent de **désactiver** le MFA.  
Nomenclature du groupe : GRP-XXX-SVC
- Les utilisateurs rencontrant un **problème** avec leur MFA peuvent être placés dans des **groupes** d'exclusion **temporaires**.  
Nomenclature du groupe : GRP-XXX-TMP-EXCLUDE-MFA

Lors de la notification MFA, l'utilisateur peut **signaler** qu'il n'est pas à l'origine de la demande de connexion. Le compte est dès lors considéré comme **potentiellement compromis**, car un attaquant est peut être en possession des identifiants de l'utilisateur. La connexion est alors **considérée** comme une **fraude**, et l'utilisateur voit son **compte bloqué**.

Afin de le **débloquer**, après vérification de l'origine de la demande **avec** l'utilisateur, un **ticket** doit être ouvert à destination de l'équipe centrale **Microsoft 365 / Identité** qui pourra débloquer le compte.

Si l'utilisateur n'est effectivement **pas** à l'origine de la demande de connexion, la fraude est **avérée** et le compte est considéré comme **compromis**. Le compte utilisateur est alors **automatiquement bloqué** ; le **mot de passe** doit être **changé** et les **sessions de connexion** doivent être **révoquées** immédiatement.

### ► RESSOURCES

Nom de l'indicateur	Description	Périodicité	Cible
Temporary Exclusion Count	Nombre de comptes présents dans le groupe d'exclusion temporaire	Hebdomadaire	0
Temporary Exclusion Time	Temps passé des comptes dans le groupe d'exclusion temporaires	Hebdomadaire	0

Retrouvez le fichier de support pour utilisateurs vers le lien suivant :

*Si vous n'avez pas accès au document, veuillez en faire la demande*

Lien

# Accès conditionnels



Périmètre  
VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation  
Inclus dans les licences utilisateurs



Contrat  
VINCI

## 4.5 | Accès conditionnels

### ► DESCRIPTION

L'accès conditionnel est un système qui vérifie les conditions d'accès aux systèmes d'information (Qui ? Où ? Type de PC). Si ces conditions ne sont pas remplies, l'accès de l'utilisateur aux données est réduit, modifié ou bloqué.

### ► RÈGLES



#### Pour tout le monde



##### Cyber-passport

*Si vous ne passez pas votre cyber-passeport\**

- Vous devrez vous reconnecter à votre compte Microsoft 365 **toutes les 24 heures** et vous serez notifié d'une durée d'utilisation spécifique.

*\* La réussite du cyber-passeport est obligatoire pour accéder au système d'information, vérifiez auprès de votre département RH pour l'affectation - Ceci s'applique également aux nouveaux arrivants.*



##### Pays approuvé

*Si vous êtes en Iran, au Nigeria, en Corée du Nord ou en Russie*

- Votre accès à votre compte et donc aux applications en nuage telles que Microsoft 365 sera **bloqué**.



##### PC

*Si vous utilisez un PC de construction non VINCI / un PC VC non conforme*

- Vous ne pouvez seulement vous connecter aux applications en ligne que par l'intermédiaire du navigateur (le client lourd n'est pas autorisé).
- Vous devrez vous connecter toutes les **24 heures\***



##### Téléphone

Seules les applications Microsoft sont autorisées à accéder aux données VC, comme Outlook mobile pour consulter vos courriels.

Vous devrez vous connecter toutes les **24 heures** (uniquement pour l'utilisation en ligne de Microsoft 365, pas pour les applications).

Un code PIN sera demandé pour accéder aux outils M365.

*Sur les téléphones non mis à jour ou téléphones Windows*

- Vous n'aurez pas accès à votre compte et donc aux données de VC



#### Orienté vers les profils informatiques



##### Compte Administrateur

*Si vous disposez d'un compte privilégié, tel qu'un compte ADT\_*

- La première fois que vous vous authentifiez, il vous sera demandé de signer les chartes administratives de VINCI.
- Vous ne pourrez vous connecter à votre compte qu'à partir d'un appareil VINCI Construction

Rule #1	You will have to sign-in every <b>24 hours</b>
Rule #2	You must use a VC computer

\* Seulement les PC non VINCI

# Référentiel d'architecture

NEW



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation  
IT Fees



Contrat  
VINCI Construction

## 5.2 | Référentiel d'Architecture

### ► DESCRIPTION

 MAPPIFY offre, depuis janvier 2024, une description des **informations** (Objet Métier) opérées par les Métiers au travers d'**Applications** et d'**Interfaces** dans les **Processus métier** de chaque **Domaine The Way We Work** de VINCI Construction.

Le S.I. évolue constamment et MAPPIFY permet de suivre son **évolution** en « temps réel » et de constater son **état de santé**. MAPPIFY permet entre autres de visualiser à un instant donné l'**impact** qu'aura toute évolution ou panne dans le S.I., quelle que soit la couche Métier, Fonctionnelle, Applicative ou Technique touchée.

Le référentiel d'architecture MAPPIFY, c'est l'affaire de chacun au sein de VINCI Construction.

### ► RÈGLES

#1 Tout Collaborateur VINCI Construction accèdera au référentiel publié dès Juillet 2024.



#2 Tout Collaborateur IT peut mettre à jour le Référentiel d'Architecture (dans la limite de ses responsabilités et au fil des déploiements).



Si vous n'y accédez pas, faites-en la demande dans  mySupport.

#3 Les responsables de Processus doivent mettre à jour leurs processus validés dès que ceux-ci évoluent.

#4 Si un Objet métier semble absent du référentiel, une demande d'ajout doit être effectuée dans mySupport ou MAPPIFY Portal afin que les Architectes S.I. puissent l'analyser avec vous et l'ajouter si nécessaire.

#5 Si une Application semble absente du référentiel publié sur le portail ou vous semble incomplète, une demande d'évolution de contenu dans MAPPIFY Portal ou mySupport doit être effectuée afin qu'un Architecte S.I, le Product Owner ou l'IT Lead puisse procéder au complément.

#6 En tant que Product Owner, IT Lead, équipe de développement ou interlocuteur Infrastructures & Opérations, il est de votre responsabilité de vous assurer que toute évolution soit tracée dans ce référentiel, ce qui facilitera le travail de toutes les équipes tant pour la maintenance de notre S.I. que pour son évolution et leur permettra de voir plus clairement les roadmaps DSI se dessiner.



### ► RESSOURCES

Dans le tableau ci-dessous, vous retrouverez l'ensemble des objets S.I. suivis dans les versions de MAPPIFY :

	Objet Référentiel	Dans le Référentiel	Publié sur le Portail
Couche Métier	<b>Processus Métier</b>	V2 – Janvier 2024	V2 – Juillet 2024
	<b>Objet Métier</b>	V2 – Janvier 2024	V2 – Juillet 2024
	<b>Bloc fonctionnel (Urbanisme)</b>	V2 – Janvier 2024	V2 – Juillet 2024
	<b>Flux fonctionnel</b>	V2 – Janvier 2024	V2 – Juillet 2024
Couche Applicative	<b>Application</b>	V1 – Novembre 2023	V2 – Juillet 2024
	<b>Technologie logicielle</b>	V1 – Novembre 2023	-
	<b>Service applicatif</b>	V2 – Janvier 2024	V2 – Juillet 2024
Couche Technique	<b>Middleware</b>	V2 – Janvier 2024	-
	<b>Service technique</b>	V3 – Septembre 2024	-
	<b>Composant infrastructure</b>	V3 – Septembre 2024	-
	<b>Composant technique</b>	V3 – Septembre 2024	-

# 5 | Support

1. Accompagnement sur les outils collaboratifs et bureautiques
2. Accompagnement au changement
3. Négociation et suivi de contrat IT
4. Offre UX
5. Sécurité dans les projets IT

### Accompagnement sur les outils collaboratifs et bureautiques



**Périmètre**  
Tout VINCI Construction



**Statut**  
Modular



**Dernière mise à jour**  
Mars 2024



**Facturation**  
A étudier au cas par cas



**Contrat**

-

## 5.1 | Accompagnement sur les outils collaboratifs et bureautiques

### ► DESCRIPTION

Les accompagnements des utilisateurs **dans l'usage et la maîtrise des outils** collaboratifs et bureautiques, sont proposés **sur le portail myHelp** :

- **Des ressources documentaires** sous des formats variés :
  - sur les outils Microsoft 365 autour de l'organisation individuelle, la collaboration d'équipe et la communication à large échelle
  - sur les outils de cybersécurité, de signature, de stockage/archivage, du bureau (PC) et en mobilité
  - Des trucs et astuces et bonnes pratiques digitales
- **Des accompagnements à la carte** :
  - parcours individuels en ligne : découverte, fondamentaux et avancés
  - sessions live planifiées ou en replay « Office Cafés »
  - coachings collectifs d'équipe sur des besoins spécifiques ou cas métier jusqu'à une session « Digital Office Day » pour un site
  - programme ambassadeurs/référents



myHelp

### ► RÈGLES

Les principes concernant les accompagnements sont les suivants :

	Parcours individuel	Office Café	Coaching collectif d'équipe	Digital Office Day
Modalité	Distanciel Lecture et replay	Distanciel En live ou replay	Hybride En live (env. 2h)	Présentiel En live (1 journée)
Thèmes	Essentiels par niveau, à suivre à son rythme	Nouveaux outils, usages, rappels ou approfondissements	Besoin spécifique sur des outils et usages (cohérence équipe)	Besoin spécifique sur des outils et usages (multi sujets et profils)
Prérequis	Aucun	Programmation définie en central	Cadrage en amont pour un déroulé spécifique	Cadrage en amont pour un déroulé spécifique
Inscription	<a href="#">Accéder aux replays</a>	<a href="#">Inscription</a>	A la demande	A la demande

Pour tout déplacement, le nombre de participants doit être d'au moins **10 personnes**.

Vous pouvez contacter l'équipe à l'adresse suivante : [digitaloffice@vinci-construction.com](mailto:digitaloffice@vinci-construction.com).

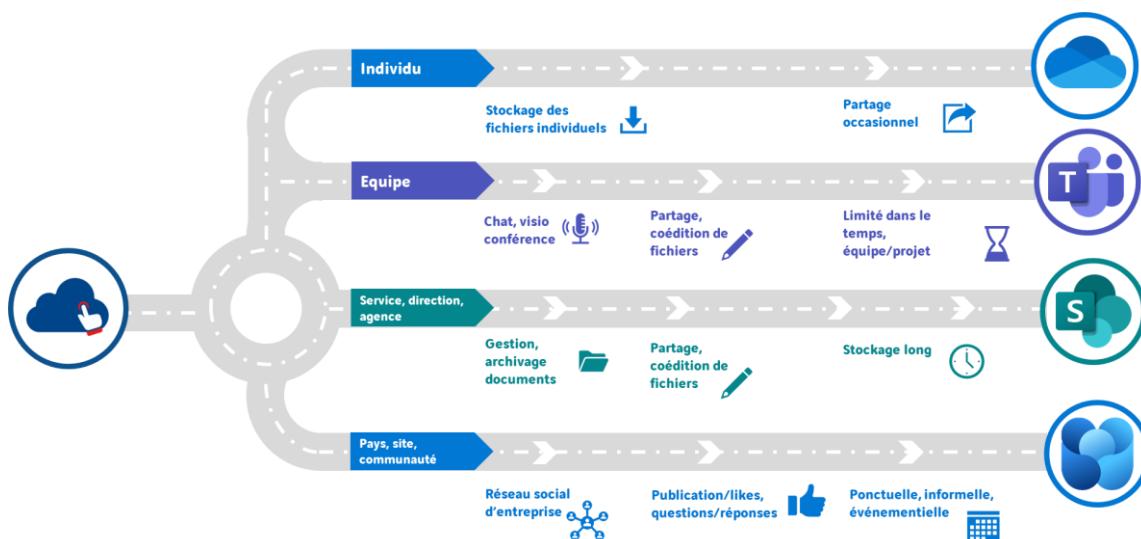
Le programme ambassadeurs/référents est en cours d'élaboration.

SUPPORT

SUPPORT

### ► RESSOURCES

Un exemple de **ressources** mis à disposition sur le portail **myHelp** : Quel outil pour quels usages ?



# Accompagnement du changement



**Périmètre**  
Tout VINCI Construction



**Statut**  
Modular



**Dernière mise à jour**  
Juin 2023



**Facturation**  
A étudier au cas par cas



**Contrat**  
-

## **5.2 | Accompagnement du changement**

## ► DESCRIPTION

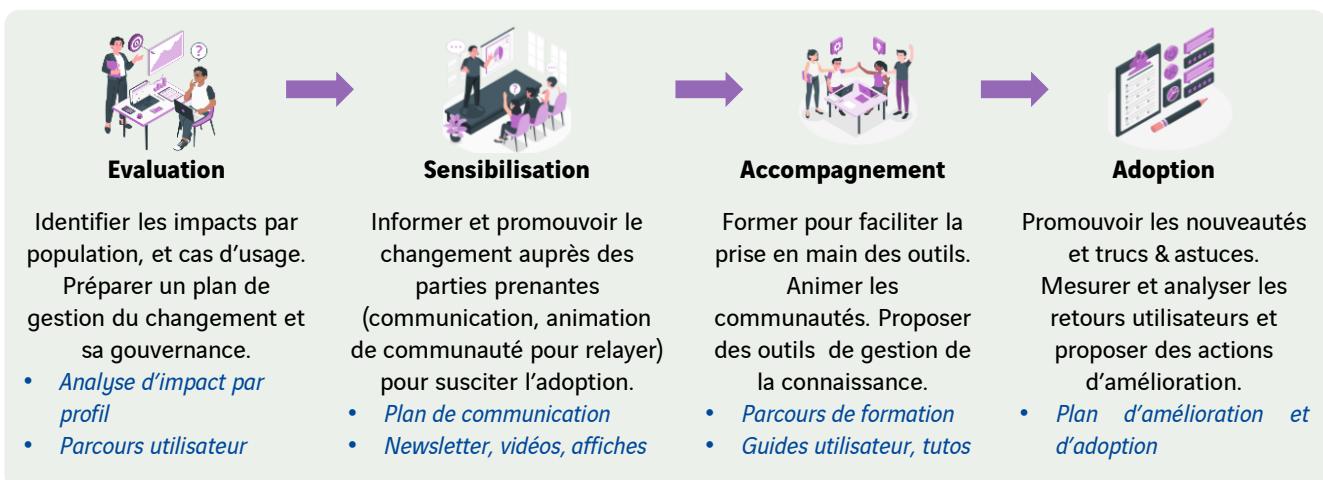
Notre mission consiste à vous accompagner dans la **conduite du changement** de vos projets IT, en vue de faciliter l'**adoption** de la solution mise en place.

Notre démarche vise à **analyser** et **qualifier** les **changements** induits et leurs impacts, à mettre en place des dispositifs d'**accompagnement** et enfin à **ancrer** le changement. Car on considère que la conduite du changement repose sur **trois** grands piliers :

- Comprendre les enjeux du changement
  - Communiquer sur le changement
  - Bien vivre le changement

## ► RÈGLES

**La conduite du changement intervient de bout en bout du cycle de vie du projet IT :**



Pour toute question ou demande d'information, vous pouvez contacter l'équipe à l'adresse suivante :  
[IT\\_changeandUX@vinci-construction.com](mailto:IT_changeandUX@vinci-construction.com)

Une prise de contact nous permettra d'échanger sur votre besoin. Des ateliers de cadrage seront programmés afin d'analyser les impacts et construire le plan de Conduite du Changement adapté au projet IT.

## ► RESSOURCES

Voici quelques exemples de livrables :

A slide titled "Challenges" featuring the Vinci logo. It includes a QR code and a circular graphic with a recycling symbol and the text "Alliez votre espace digital à l'écologie". Below the slide is a call to action: "Triez et supprimez le plus de données obsolètes !".

## Vidéos

# Questionnaires de satisfaction

Enquête de Satisfaction - Sessions Digital Office

Vous avez participé à une session Digital Office et nous vous en remercions !  
 Nous aimons recevoir votre avis sur l'environnement et son contenu.  
 Merci de prendre quelques minutes pour répondre nos questions.

\* Obligatoire

1. Adresse e-mail \*

Entrez votre réponse

## Négociation et suivi de contrat IT



**Périmètre**  
Tout VINCI Construction



**Statut**  
Modular



**Dernière mise à jour**  
Mars 2024



**Facturation**  
A étudier au cas par cas



**Contrat**  
VINCI Construction

## 5.3 | Négociation et suivi de contrat IT

### ► DESCRIPTION

Afin d'accompagner les achats IT, l'équipe Contrats IT de la DSI Pôle propose un service d'accompagnement dédié durant la négociation d'un contrat IT.

Cet accompagnement permet principalement :

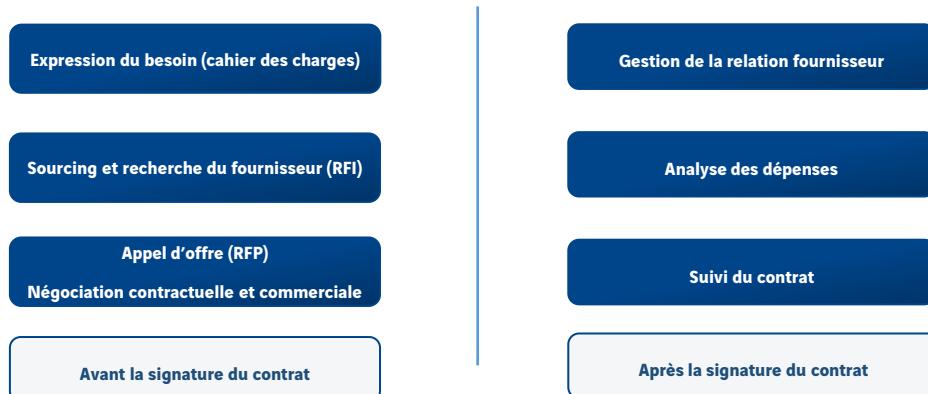
- De préserver les intérêts de VINCI Construction en négociant les clauses juridiques et les conditions contractuelles (Qualité, Coûts et Délais).
- D'apporter un gain de temps et permettre aux managers de se concentrer sur leur cœur de métier.
- De pérenniser la relation commerciale et préserver la qualité de la prestation sur le long terme.
- D'apporter une connaissance IT dans ce cadre.

Cette offre couvre les domaines suivants :

- Achats de matériel
- Licences
- Prestation de services IT

### ► RÈGLES

L'accompagnement peut intervenir avant ou après la signature du contrat ; voici les étapes clés :



Pour bénéficier d'un accompagnement, vous pouvez vous adresser à l'équipe Contrats IT à l'adresse suivante : [it-contracts@vinci-construction.com](mailto:it-contracts@vinci-construction.com)

### ► RESSOURCES

Une boîte à outils achats regroupant des modèles de documents pouvant servir durant l'ensemble des étapes du processus achats est disponible :

The image shows a screenshot of a digital tool titled "Equipe IT Contracts Boîte à outils & accompagnement". It features two main sections: "DEBLAIS DE CONSULTATION" and "FICHES DE RÉFÉRENCE". The "DEBLAIS DE CONSULTATION" section contains a form for "Demande de consultation" with fields for "Objet de la demande", "Type de document", "Référence de la demande", and "Date de validité". It includes a "REMARQUE" section with checkboxes for various requirements like "L'offre doit être claire et précise", "Le fournisseur doit pouvoir donner toute la nécessaire", etc. The "FICHES DE RÉFÉRENCE" section contains three tables: "Variables", "Paramètres / Catalogue", and "Options". Each table has columns for "Nom", "Type de variable", "Valeurs possibles", and "Commentaires". At the bottom, there are sections for "TOTAL SANS OPTIONS" and "OPTIONS".

## Offre UX



**Périmètre**  
Tout VINCI Construction



**Statut**  
Modular



**Dernière mise à jour**  
Mars 2024



**Facturation**  
A étudier au cas par cas



**Contrat**

-

## 5.4 | Offre UX

### ► DESCRIPTION

#### Qu'est-ce que l'expérience utilisateur (User eXperience) ?

L'UX désigne la qualité de l'interaction entre les utilisateurs et une interface graphique (application, site, etc.).

#### Comment notre offre UX peut-elle vous aider ?

Nous vous accompagnons dans l'amélioration ou la création de vos interfaces graphiques.

#### Pourquoi inclure l'UX à vos projets ?

L'objectif est d'assurer la satisfaction des utilisateurs, en les plaçant au centre des projets et en garantissant la simplicité, la lisibilité, la satisfaction, la cohérence, l'attractivité et l'accessibilité des interfaces.

### ► RÈGLES

La méthodologie est adaptée selon les besoins et les contextes :



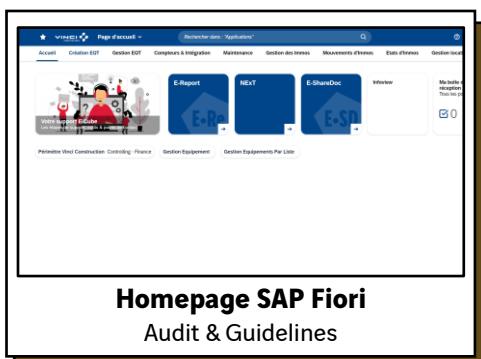
Exemple d'accompagnement :

Méthode	Description	Livrable
<b>Audit ergonomique</b>	Vérifier la facilité d'usage de l'interface. Déterminer les irritants pour les utilisateurs.	Rapport des irritants avec les recommandations d'amélioration.
<b>Évaluation de la satisfaction utilisateurs</b>	Enquêter utilisateurs (interview, questionnaire ou focus group) pour obtenir leur satisfaction, remarques et besoins.	Questionnaire, résultats, interprétation et recommandations.
<b>Atelier d'idéation</b>	Stimuler la créativité au sein d'un groupe de travail.	Idées innovantes, parcours utilisateurs, besoins utilisateurs.
<b>Maquettage et organisation de l'information</b>	Créer des maquettes ou prototypes des futures interfaces. Structurer le contenu sous forme d'arborescence.	Arborescence de contenu, maquettes et prototypes.
<b>Tests utilisateurs</b>	Évaluer l'interface en la faisant tester à un panel d'utilisateurs.	Rapport chiffré (taux d'erreur, clics, temps de navigation), verbatims et recommandations d'amélioration.

Contactez-nous : [IT.changeandUX@vinci-construction.com](mailto:IT.changeandUX@vinci-construction.com)

### ► RESSOURCES

#### Quelques-uns de nos projets :



**Homepage SAP Fiori**  
Audit & Guidelines



**Intranet SharePoint ONE Finance**  
Idéation & Maquettage

#### Nos outils :



# Sécurité dans les projets IT

NEW



Périmètre  
Tout VINCI Construction



Statut  
Local



Dernière mise à jour  
Septembre 2024



Facturation  
IT Fees



Contrat

SUPPORT

SUPPORT

## 5.5 | Sécurité dans les projets IT

### ► DESCRIPTION

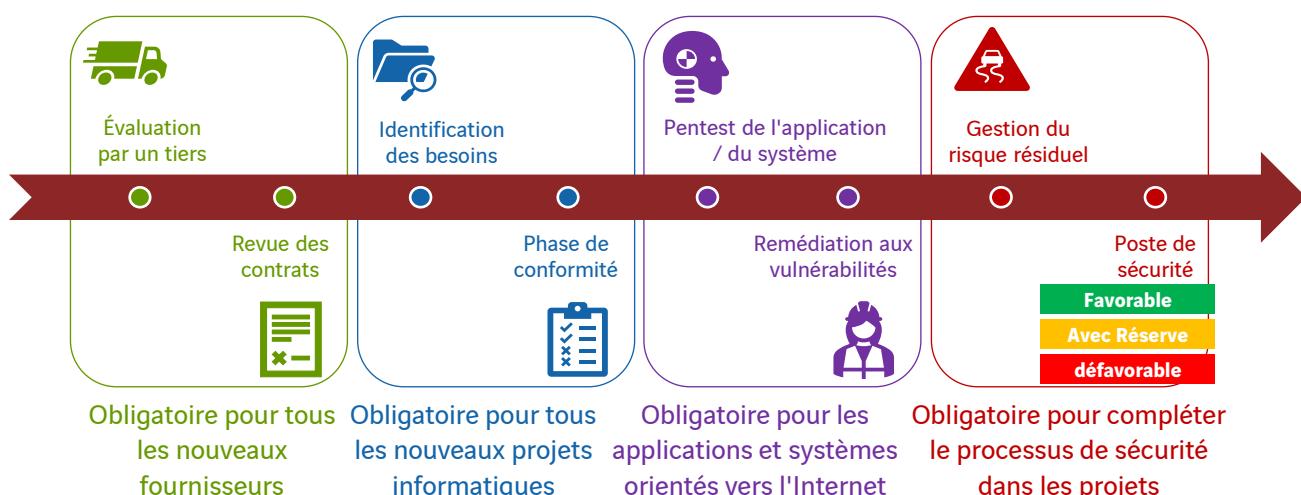
L'intégration de la sécurité dans les projets informatiques est un élément fondamental de **Security by design**. Elle garantit que la cybersécurité est incluse dans le **cycle de vie des solutions informatiques** conçues par VINCI Construction.

### ► RÈGLES

La sécurité des projets informatiques est **gérée localement** au niveau de la division ou du pays.

- Si un pays ou une division est totalement autonome du point de vue de la cybersécurité, il doit contacter **le RSSI local** et n'a pas besoin de contacter la VCSI.
- Si un pays ou une division n'a pas de **responsable informatique local**, il peut contacter le RSSI du groupe.

Les divisions disposant des moyens techniques peuvent prendre en charge les pentests, sinon la VCSI peut offrir un service qui sera facturé.



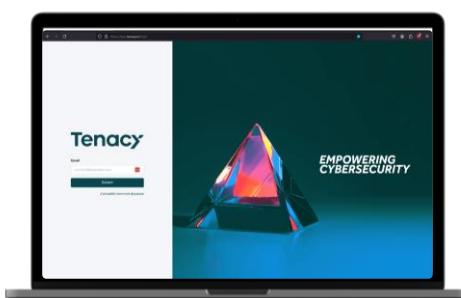
### ► RESSOURCES

SUPPORT

Pour gérer la sécurité dans les projets informatiques, VCSI a choisi **Tenacy comme outil de soutien**.

#### Un outil pour la gestion

- L'évaluation
- Conformité
- Dérogation
- Actions
- Indicateurs



Pour toute question ou demande d'accès à Tenacy, veuillez contacter l'équipe Cybersécurité via **mySupport**.

Des informations supplémentaires (fichiers de contrat/Tenacy) sont disponibles sur le SharePoint Security by Design : [Security by design](#)

SUPPORT

# 6 | Organisation

1. Ressources IT
2. UNITY Service Book
3. Support utilisateur
4. IT Service Management (ITSM)
5. Facturation des coûts IT

# Ressources IT



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation  
IT Fees



Contrat

## 6.1 | Ressources IT

### ► DESCRIPTION

Cette fiche de service vise à décrire les espaces clés mis à disposition niveau Pôle, et la gestion de la connaissance associée.

### ► RESSOURCES NEW



#### Accessible à tous



##### The Way We Work

Présentation **du langage commun et des règles** VINCI Construction, par domaine.



##### myHelp

**Portail d'aide en ligne** des applications, M365 et autres outils.



##### mySupport

**Outil** de la chaîne de support IT (incident ou faire une demande de service, ...).



##### ONE

**Site intranet groupe** de certaines entités de VINCI Construction.



##### Espace ONE IT

Retrouvez les actualités, l'organisation, les liens utiles.



##### Trombinoscope des équipes VCSI



##### Coûts IT

**Coûts & refacturation** des services IT.



#### Orientés profils IT



##### VC IT Network SharePoint

Bibliothèque des **documents IT clés** dans la coordination DSI Pôle et Divisions/Pays.



##### IT KPI



Présentation des **statistiques liées aux SI**: licences Microsoft, usages des outils M365, % de passage du Passeport Cybersécurité...



##### IT Book

Présentation des **services IT VINCI Construction et règles associées**



##### PC/ Smartphone Catalogue

Catalogue commun et adaptable par chaque Division

# UNITY Service book



Périmètre  
Tout VINCI Construction



Statut  
Local



Dernière mise à jour  
Mars 2024



Facturation

-



Contrat

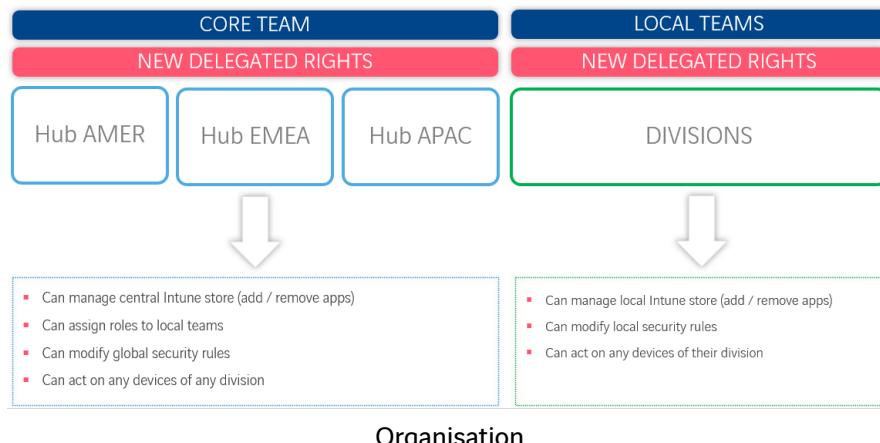
-

## 6.1 | UNITY Service book

### ► DESCRIPTION

**UNITY** est un service global à VINCI Construction et opéré mondialement. Les règles communes sur les mobiles et les postes de travail sont définies et gérées par l'équipe « **CORE** » avec des représentants dans chaque plaque géographique (organisation follow-the-sun).

Les **Equipes locales** ont l'autonomie pour gérer leurs équipements dans la console Intune et appliquer des configurations ou applications localement tant que cela n'est pas en conflit avec les règles ou standards de sécurité communs.



### ► RÈGLES

Le **UNITY Service Book** contient l'ensemble des règles s'appliquant aux équipes de support « **Core** » et « **Local** »

Règles « **Core team** » :

#	Description
R-1	Les membres de la core team (CT) sont nommés par les CIOs de division
R-2	La CT est localisée dans 3 hubs géographiques, AMER, EMEA, APAC
R-3	La CT offre du support L3 pour toutes les divisions dans chaque hub
R-4	La CT régionale peut gérer les incidents régionaux de manière indépendante
R-5	La CT est responsable d'organiser les comités de gestion d'Intune
R-6	La CT est responsable de la gestion et l'implémentation des changements globaux
R-7	La CT aura accès à tous les équipements présents dans Intune (Poste de travail & mobiles)
R-8	Il n'y a pas de séparation dans l'information au niveau central
R-9	Les membres de la CT doivent être expérimentés et certifiés Microsoft MD-102

Règles « **Local team** » :

#	Description
R-1	La Local Team (LT) regroupe des membres des équipes IT L1 & L2 de chaque division
R-2	La LT est responsable du support UNITY L1 et L2
R-3	La LT est responsable de communiquer localement sur les interruptions de service
R-4	La LT est responsable d'escalader les incident L3 à la CT régionale à travers l'outil ITSM
R-5	La LT n'a accès qu'aux équipements de sa division
R-6	Les membres de la LT ont accès au management des PC et des mobiles de leur division

### ► RESSOURCES NEW

Lien vers UNITY  
Service Book

\* L'accès au UNITY Service Book est accessible à toutes les divisions.

# Support utilisateur



Périmètre  
Time Zone France



Statut  
Modular



Dernière mise à jour  
Septembre 2024



Facturation  
IT Fees



Contrat

## 6.3 | Support utilisateur

### ► DESCRIPTION NEW

Premier point de contact pour le collaborateur, le **Service Desk** fournit des services IT pour résoudre :

- Les **incidents** (interruption du service IT partielle ou totale, pour un ou plusieurs utilisateurs)
- Les  **demandes de service** (ex : création des comptes d'un nouvel arrivant, accès à des ressources réseaux, installation de logiciels, etc.)

Il opère la répartition et l'escalade des tickets aux autres **groupes de support** et leur **prise** en charge.

Il garantit la  **traçabilité** et la **réactivité** pour la résolution des incidents.



### Différents accès selon le périmètre :

Ce tableau présente les différents moyens proposés aux utilisateurs pour contacter leur support en fonction de leur périmètre.

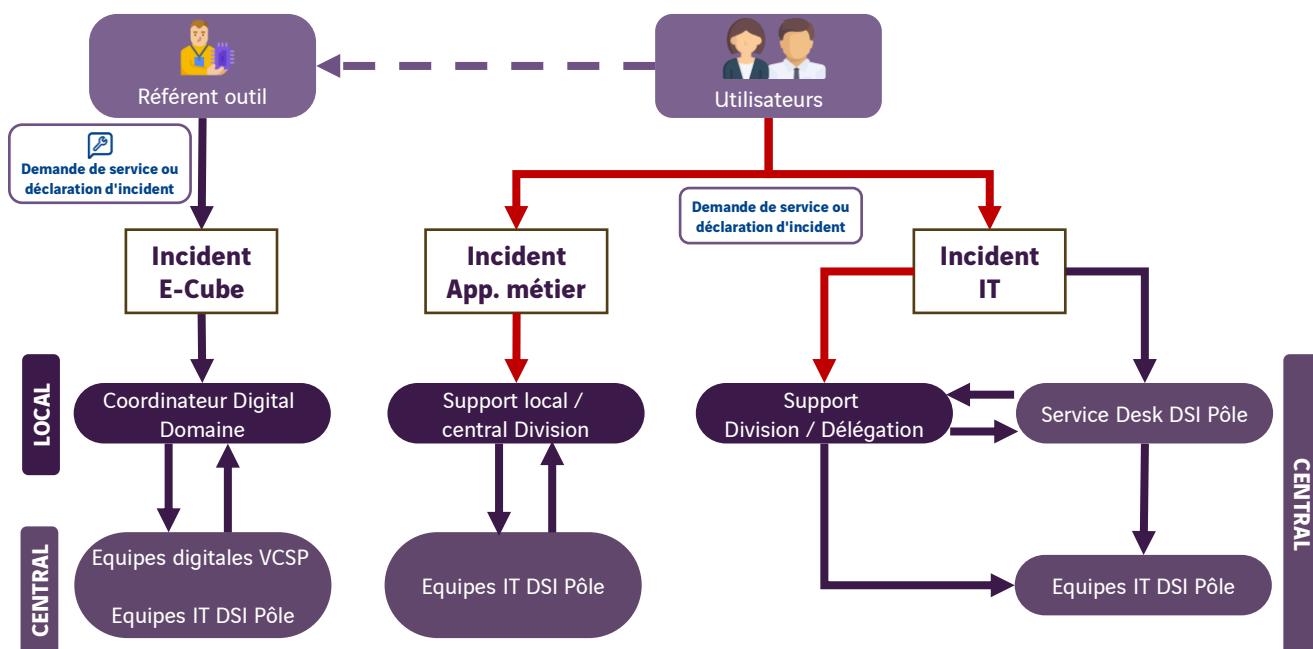
Division	Périmètre	Portail d'aide en ligne	Adresse mail	Horaires locaux d'ouverture	Numéro de téléphone
Réseaux de spécialité	-	mySupport	servicedesk@sf-group.com	Selon la plateforme et le fuseau horaire : Worldwide coverage by SEIT	
Grands Projets	Holding	mySupport	itsupport@vinci-construction.com	-	+33 1 47 16 46 76
	Dodin Campenon Bernard	Local	servicedesk@dcb-si.com	-	+33 5 62 74 80 40 option 8
Europe Afrique	-	mySupport	-	8h - 17h ouvert 4j/7 Vendredi: 8h - 15h	-
Royaume-Uni	-	Local	-	7h - 18h Ouvert 5j/7	-
Amérique Océanie	Australie	Local	servicedesk@seymourwhyte.com	7h - 17h Ouvert 5j/7	+61 7 3386 3222
	Canada	mySupport	-	5h - 20h Ouvert 5j/7	-
	Chili	Local	dinformatica@bitumix.cl	9h - 18h30	-
	Nouvelle-Zélande	mySupport	helpdesk@heb.co.nz	07h-18h ouvert 5j/7	-
	Etats-Unis	Local	-	Ouvert 24x7	1-866-936-4040
France Génie Civil France Bâtiment	-	mySupport	servicedesk.vcf@vinci-construction.com	8h-18h ouvert 5j/7	+33 1 41 91 48 48
France Réseaux France Route	-	mySupport	itsupport@vinci-construction.com (Sogea, TTMF) 4040@vinci-construction.com	8h-18h ouvert 5j/7	+33 1 47 16 40 40
Siège	VCSP / VCSI	mySupport	itsupport@vinci-construction.com	8h-19h ouvert 5j/7	+33 1 47 16 46 76

## 6.3 | Support utilisateur

### ► DESCRIPTION (suite)

#### Fonctionnement de la chaîne de support :

Ce schéma décrit la chaîne de support selon les périmètres et les applications concernés :



- L'utilisateur contacte son référent outil local habilité à créer un ticket dans mySupport Pour plus d'informations sur la chaîne de support E-Cube, veuillez consulter [myHelp](#)
- Ticket géré exclusivement via mySupport
- Ticket créé directement dans mySupport ou dans l'outil de support local puis recréé dans mySupport si besoin d'intervention du support central

### ► RÈGLES

L'adresse mail [international.itsupport@vinci-construction.com](mailto:international.itsupport@vinci-construction.com) ne doit être utilisée que par les **IT Divisions/IT managers internationaux** pour contacter directement le support en central. Une équipe dédiée de la DSi pôle a la charge de gérer les tickets qui proviennent de l'international (ouvert 5j/7 de 8h à 19h, UTC+01:00 - Heure de Paris).

Tout doit passer par les canaux prévus à cet usage **décrits dans le tableau précédent** pour garantir la traçabilité des demandes.

Il est **interdit d'écrire directement** à un agent du Service Desk ou d'utiliser une liste de diffusion du Service Desk.

### ► RESSOURCES

- Le glossaire OPTIM (Optimisation du Processus de Traitement des Incidents Majeurs) : [Glossaire OPTIM](#)
- mySupport Front Office : <https://mysupport.easyvista.com/s/mysupport>
- mySupport Back Office : <https://mysupport-back.easyvista.com/> (pour les opérateurs IT uniquement)

# IT Service Management (ITSM)



Périmètre  
Tout VINCI Construction



Statut  
Local support: Modular  
Core applications support: Core



Dernière mise à jour  
Mars 2024



Facturation  
IT Fees



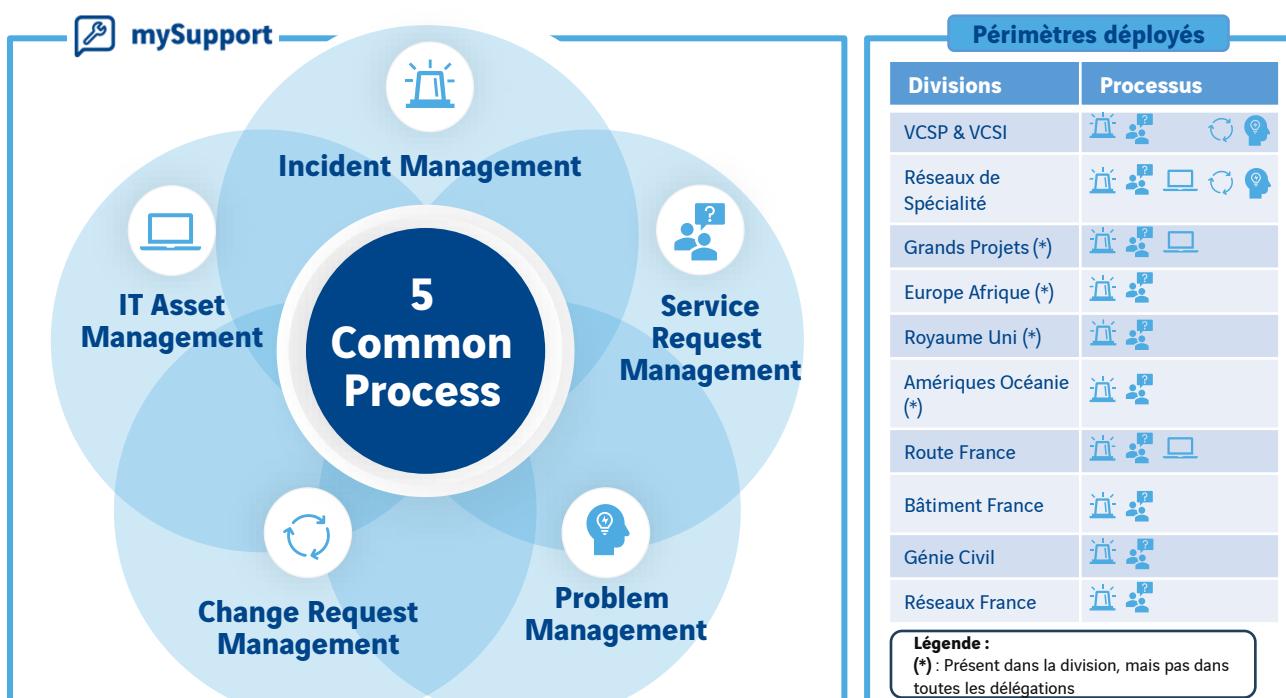
Contrat  
VINCI

## 6.4 | IT Service Management (ITSM)

### ► DESCRIPTION

L'outil ITSM de VINCI Construction est **mySupport**. La solution est disponible en plusieurs langues : Français / Anglais / Espagnol et Allemand. mySupport est portée par la solution **EasyVista** qui est la solution ITSM VINCI. mySupport est utilisé par l'ensemble de VINCI Construction pour faire le lien entre les Divisions vers le support de la DSI Pôle, est déployé systématiquement dans le cadre E-Cube/Connect@ et est recommandé pour le support local.

L'outil ITSM supporte les processus de la chaîne de support IT (incidents, demandes de services, etc...). Il permet de tracer l'activité et les interactions entre les **utilisateurs** et les **opérateurs**, et de fournir le reporting global de l'activité de support.



Le service ITSM se compose de 3 parties distinctes :

- **Le Front Office** : le portail **utilisateur** permet à tous les utilisateurs identifiés de déclarer un incident ou de faire une demande à partir du catalogue de service.
- **Le BackOffice** : le portail **opérateur** permet les traitements des tickets ou création par les opérateurs si nécessaire.
- **Le Reporting** : il donne accès au suivi d'activité support soit directement dans mySupport, soit via un dashboard additionnel dédié.



## 6.4 | IT Service Management (ITSM)

### ► RÈGLES

#### Accès à l'ITSM

Pour accéder à l'ITSM il faut avoir un compte VC et être déclaré dans les référentiels VINCI Construction. Pour accéder au backoffice, il faut de plus demander un profil opérateur.

#### Règles Communes et spécifiques :

La solution partage des **règles communes** comme la structure des catalogues, le nommage des groupes, les référentiels, les règles d'assignation, ... .

La solution propose des catalogues pour gérer les éléments comme les incidents, les demandes de service, les équipements.

**Le catalogue CORE est commun à tous les périmètres.** Il est défini avec l'ensemble des référents et Il est géré par l'équipe centrale.

**Chaque division ou délégation peut ensuite avoir des catalogues spécifiques.**

**Chaque périmètre est responsable de son catalogue** et peut ainsi en définir la visibilité et l'assignation en fonction des sujets.

#### Le modèle d'administration fédérée :

- L'outil ITSM est **maintenu et administré par l'équipe centrale de la DSI Pôle.**
- Les Divisions ont également un rôle dans la gestion de la solution (Administrateur et/ou Expert) :

Administrateur	Expert
Tâche d'administration basique du périmètre	Tâche d'administration basique Développement en environnement de test
<b>Prérequis :</b> Formation Interne d'Administration	<b>Prérequis :</b> Formation Interne d'Administration Formation éditeur sur la solution.

### ► RESSOURCES

Nom	Description	Langues
<b>myHelp</b> : ( <a href="#">lien</a> )	Site de référence des documents et connaissances relatifs à mySupport	FR/EN
<b>Viva Engage mySupport</b> ( <a href="#">lien</a> )	Site de la communauté mySupport pour suivre l'actualité	FR/EN

# Facturation des coûts IT



Périmètre  
Tout VINCI Construction



Statut  
Core



Dernière mise à jour  
Septembre 2024



Facturation

-



Contrat  
VINCI Construction

## 6.5 | Facturation des coûts IT

### ► DESCRIPTION

Tous les services fournis par la VCSI sont facturés aux Divisions, pays ou Délégations (y compris les services non encore présents dans l'IT Book). Les coûts IT sont définis en trois catégories :



Les **Fees** sont le % de Chiffre d'Affaires payé par une entité (Division, pays ou Délégation) en fonction notamment de son ERP et des outils de gestion déployés.



#### Autres coûts :

**COST PER UNIT**: basés sur les usages (logiciels, hébergements...)

**COST PER SERVICE**: définis à l'avance (prestations sur devis ou convention)

### ► RULES

Les **règles de facturation** font l'objet d'une **note officielle diffusée en début de chaque année** par le Directeur de la DSI et la Direction du contrôle de gestion de VINCI Construction. Ces règles sont communiquées chaque année. Les devis et les factures sont envoyées par la DSI VINCI Construction.

Les **règles de facturation à l'intérieur des Divisions ou entités** sont propres à chacune d'elles.

#### Planning type de facturation des coûts IT :

T1	T2	T3	T4
<b>15/01</b> Note officielle publiée	<b>30/06</b> <b>COST PER UNIT</b> Extraction des licences utilisateurs M365	<b>01/09</b> Devis <b>COST PER UNIT</b> et <b>COST PER SERVICE</b> à envoyer aux Divisions	<b>20/09</b> Les facture des licences utilisateurs M365 envoyées aux Divisions <b>15/11</b> Autres factures y compris Fees

**Règles de comptage des licences M365** : elles sont comptées et extraites le 30 juin puis ce nombre est considéré comme la moyenne des licences sur l'année.

#### Règles appliquées pour les autres services:

- **FEES** : le barème est validé par le COMEX de VINCI Construction.
- **COST PER SERVICE** : les coûts sont basés sur un accord entre la DSI pôle et les entités.
- **COST PER UNIT** : le catalogue de prix communiqué pendant l'année A-1 et partagé avec les entités sur la base de métriques (utilisateurs, VM, BU,...).

Les factures sont envoyées par le service comptable de la DSI pôle aux Directeurs Administratif et Financier de chacune des entités désignées par le contrôle de gestion de VINCI Construction holding.

L'IT Pole peut fournir les justifications de usages des services.

### ► RESOURCES

Pour plus de précisions :



Coûts IT