

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	1/12

Direction du Système d'Information

Contexte informatique d'IFP Energies nouvelles

But de l'instruction :

Cette instruction a pour objectif de décrire le contexte informatique d'IFP Energies nouvelles dans lequel doivent s'intégrer les réponses aux appels d'offres d'IFP Energies nouvelles et les contraintes associées qui doivent être respectées.

Les éléments de cette instruction ont vocation à être intégrés en annexe technique des cahiers des charges des appels d'offres.

Champ d'application :

Ensemble des consultations concernant les infrastructures et les applications informatiques.

Objet de la révision :

Le présent document fait l'objet d'une révision périodique pour tenir compte de l'évolution de l'environnement informatique d'IFP Energies nouvelles.

Rédaction Nom / visa	Vérification Nom / visa
Date 19/03/2024 Responsable du pôle Architecture	Date : 19/03/2024 Urbaniste SI

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	2/12

Direction du Système d'Information

SOMMAIRE

A CORPS DE L'INSTRUCTION	3
1 Introduction.....	3
2 L'environnement informatique d'IFP Energies nouvelles	4
2.1 Cartographie technique du SI.....	4
2.2 Réseau et hébergement	4
2.3 Serveurs et stockage.....	5
2.4 Postes de travail (systèmes d'exploitation et logiciels)	6
2.5 Architectures applicatives	6
2.6 Les applications du système d'information	8
3 Contraintes et recommandations générales.....	10
4 Contraintes en matière de sécurité informatique.....	11

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	3/12

Direction du Système d'Information

A Corps de l'instruction

1 Introduction

L'environnement informatique d'IFP Energies nouvelles et les contraintes associées sont décrits dans les chapitres suivants.

Toute réponse d'un soumissionnaire à un appel d'offres d'IFP Energies nouvelles concernant une infrastructure ou une application informatique doit s'intégrer dans cet environnement et respecter les contraintes associées, dont la sécurité.

Direction du Système d'Information

2 L'environnement informatique d'IFP Energies nouvelles

2.1 Cartographie technique du SI

Les infrastructures informatiques communes à l'ensemble de l'entreprise sont décrites dans des domaines techniques.



2.2 Réseau et hébergement

Réseau et sécurité	<ul style="list-style-type: none"> • 2 sites : Rueil-Malmaison (92) et Solaize (69) • Liaison privée intersites à 2 x 10 Gb/s • Liaisons Internet : <ul style="list-style-type: none"> ○ Flux métiers <ul style="list-style-type: none"> ▪ 2 x 4 Gb/s depuis le site de Rueil-Malmaison ▪ 2x 5 Gb/s depuis le site de Solaize ○ Flux utilisateurs via un proxy ○ 1 Gb/s depuis le site de Solaize ○ P 1Gb/s depuis le site de Rueil-Malmaison • Protocole IP • Cœurs de réseau redondants 2x10Gb/s
--------------------	---

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	5/12

Direction du Système d'Information

	<ul style="list-style-type: none"> • Zone sécurisée en DMZ pour les accès extérieurs • Connexion des postes mobiles en VPN SSL • Segmentation par VLAN applicatif ou d'usage métier à l'aide de Firewall. Ouverture des flux en fonction des ports applicatifs utilisés • Reverse Proxy pour les flux internes • Reverse Proxy pour les flux externes (en DMZ)
Salle machines	<ul style="list-style-type: none"> • Les salles machine sont sécurisées et redondantes sur chaque site • Elles hébergent principalement des serveurs virtuels et du stockage • Si besoin d'intégrer des serveurs physiques ou appliances, il est nécessaire de spécifier le nombre de U nécessaires, la puissance calorifique dissipée ainsi que la puissance électrique (type de connecteur, longueur, largeur...)

2.3 Serveurs et stockage

Infrastructure de conteneurs	<ul style="list-style-type: none"> • Clusters Kubernetes 1.26 - 1.27 <ul style="list-style-type: none"> ○ Cpus max par conteneur : 48 ○ Memoire max par conteneur : 256Gb ○ Volumes persistants : Nvme, SSD et/ou Sata
Infrastructure virtuelle de serveurs	<ul style="list-style-type: none"> • Serveurs Dell ou HPE, mémoire 384 Go à 1024 Go, VMware ESXi 8.0 Enterprise Plus • Taille maximum recommandée de VM : 16 CPU, 128 Go de mémoire • Hyperviseur VMware vSphere 8 • VMs Windows 2016, 2019, 2022, Linux Red Hat Enterprise / CentOS7, Ubuntu, Debian, Rocky Linux, appliances virtuelles
Stockage	<ul style="list-style-type: none"> • S3 Netapp (Storage Grid) ou MinIO • NAS Netapp (Ontap 9.10) • SAN NetApp et Dell • McAfee for Storage
Sauvegarde	<ul style="list-style-type: none"> • Logiciel de sauvegarde : NetBackup de Symantec (8.3) <ul style="list-style-type: none"> ○ Sauvegardes incrémentales quotidiennes et hebdomadaires sur un cycle de 5 semaines ○ Sauvegarde totale semestrielle • Sur Netapp <ul style="list-style-type: none"> ○ Snapshots quotidiens

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	6/12

Direction du Système d'Information

2.4 Postes de travail (systèmes d'exploitation et logiciels)

Informatique d'entreprise (IE)	<ul style="list-style-type: none"> • PC Windows 10 64 bits (mémoire : 8 Go) <ul style="list-style-type: none"> ◦ Antivirus McAfee: ENS10.x ◦ FW: McAfee ENS 10.x
Informatique scientifique (IS)	<ul style="list-style-type: none"> • PC Windows 10 64 bits (mémoire : 16 Go ou 32 Go) <ul style="list-style-type: none"> ◦ Antivirus McAfee: ENS10.x ◦ FW: McAfee ENS 10.x • PC Linux CentOS 7, Rocky Linux 64bits
Bureautique	<ul style="list-style-type: none"> • Microsoft 365 E3(IE et IS Windows) • OpenOffice version 3.1 (Informatique technique)
Messagerie	<ul style="list-style-type: none"> • Outlook 365 • Exchange 2013 - Online • Antivirus McAfee for Exchange • Passerelles Mail : Cisco Ironport
Navigateurs Web	<ul style="list-style-type: none"> • Microsoft Edge à jour

2.5 Architectures applicatives

Politique de déploiement OnPrem	La préconisation pour le déploiement d'une application interne est l'infrastructure de conteneurs et à défaut l'infrastructure de virtualisation de serveurs.
Bases de données relationnelles	<ul style="list-style-type: none"> • PostgreSQL(serveur dédié à chaque application) • SQL Server 2017 à 2022 (serveurs mutualisés)
ETL	<ul style="list-style-type: none"> • Talend Open Studio
Outils de restitution	<ul style="list-style-type: none"> • Qlikview • QlikSense
Ordonnanceur de travaux	<ul style="list-style-type: none"> • Visual TOM 7.1 de chez Absyss
Supervision applicative	<ul style="list-style-type: none"> • Ekara
Gestion de licences	<ul style="list-style-type: none"> • Flexlm • Rlm
Logiciels serveurs http (si non porté par l'application)	<ul style="list-style-type: none"> • Nginx • Tomcat • Internet Information Server

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	7/12

Direction du Système d'Information

	La version préconisée par IFPEN est celle fournie en standard par le système d'exploitation hôte (Windows 2016 et 2019, Linux Red Hat Enterprise / CentOS 7, Rocky Linux, Debian, Ubuntu).
--	--

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	8/12

Direction du Système d'Information

2.6 Les applications du système d'information

2.6.1 Vue d'ensemble (cartographie fonctionnelle du SI)

Dans le cadre de la démarche d'urbanisation de son système d'information (SI), IFP Energies nouvelles a modélisé l'ensemble de ses activités pour construire une cartographie métier du SI. La vue d'ensemble ci-dessous présente les deux premiers niveaux de la cartographie fonctionnelle (type de domaine et domaine).

Les applications du SI (qui arrivent en support des activités métier) et les données qu'elles gèrent sont toutes positionnées sur cette cartographie au niveau 2 (domaine) ou 3 (zone d'urbanisation fonctionnelle).



Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	9/12

Direction du Système d'Information

2.6.2 Gestion des identités et des accès

Application	Progiciel	Version	Editeur
Annuaire d'Entreprise	eDirectory NIM	V8.8.8 V4.0.2	NetIQ
Gestion des comptes	Active Directory	Version 2019	Microsoft
Fédération d'identités / SSO	ADFS pour les applications OnPrem Azure AD SSO pour les applications SaaS		Microsoft

2.6.3 Quelques applications « grand public »

Application	Progiciel	Version n > n+1	Editeur
Office	M365	E3	Microsoft
Messagerie	Exchange	2013 > Online	Microsoft
PeopleSoft Finance	PeopleSoft	V9.1	Oracle
PeopleSoft RH	PeopleSoft	V9.1	Oracle
Progress	Planisware	V7	Planisware
OSCAR	Contrat'tech	5.3	Legisway
eTemptation	eTemptation	Version 6.0.0	Horoquartz
Fœderis	Fœderis	V8.08	Fœderis
GAEL	SPARK Archive Advanced Edition	1.5.09 > Eldorado	SPARK Archive
Prisme (Intranet et Extranet collaboratifs)	JPlatform	10 SP5 > SP7	Jalios
Moteur de recherche	ASF AIF	7.8 7.8	Antidot
Wikis	Mediawiki	1.16.2	Opensource
Forge logicielle	GitLab	Community Edition	Opensource

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	10/12

Direction du Système d'Information

3 Contraintes et recommandations générales

• Contraintes
Toute proposition de prestation devra s'appuyer sur les technologies ci-dessus et être compatible avec les matériels identifiés.
L'introduction d'une nouvelle technologie reste toutefois possible mais devra faire l'objet d'une argumentation et d'une validation de la part d'IFP Energies nouvelles.
L'application/le logiciel devra être compatible avec les systèmes d'exploitation des postes de travail cités ci-dessus.
L'application/le logiciel devra être compatible avec l'ensemble des navigateurs cités ci-dessus.
L'application/le logiciel sera déployé sur un serveur virtuel (sauf indication contraire particulière).
L'application/le logiciel doit pouvoir être utilisé sans nécessiter les droits d'administration en local sur le PC.
• Recommandations
Pour l'utilisation de l'application/du logiciel, aucun déploiement sur les postes clients ne doit être nécessaire, ni aucun "plug-in" additif spécifique à un environnement donné (comme les ActiveX) sur les navigateurs préconisés à IFP Energies nouvelles. Si toutefois une fonctionnalité particulière ne pouvait pas être mise en œuvre sans plug-in ou additif, elle devra être clairement identifiée.
IFP Energies nouvelles dispose d'une charte graphique, mais n'impose pas de pré-requis technique. La DSI examinera les solutions techniques proposées au cas par cas. Les écrans de l'application ou de l'outil devront être en français et optimisés pour un affichage en 1024*768. La présence d'un ascenseur horizontal est à éviter.
En cas d'utilisation d'un portail pour accéder à l'application, celui-ci devra si possible utiliser le "bandeau IFP Energies nouvelles" déclinant les priorités stratégiques de l'entreprise.
En cas de besoin de planifier des traitements liés aux applications, les actions seront réalisées dans l'ordonnanceur IFPEN et non via le gestionnaire de tâches et/ou Crontab

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	11/12

Direction du Système d'Information

4 Contraintes en matière de sécurité informatique

• Authentification
L'accès à l'application et à ses données doit être sécurisé au moyen d'un déport d'authentification vers Active Directory (LDAP ou Kerberos), qui intègre une gestion de complexité des mots de passe et une activation/désactivation automatique des comptes.
La connexion aux applications doit se faire via un mécanisme assurant le cryptage des identifiants de connexion (utilisation du protocole HTTPS pour les applications Web)
Les comptes disposant de droits privilégiés sur l'application (pouvant être créés notamment dans le cadre de l'installation) doivent respecter les exigences de sécurité au niveau du mot de passe.
La traçabilité des accès à l'application doit reposer sur un mécanisme de journalisation des utilisateurs.
L'ouverture de l'application à des utilisateurs extérieurs (hors réseau IFPEN) est conditionnée par l'utilisation d'un reverse proxy (qui sera situé en DMZ) et qui protégera les données et les autres composants de l'application situés dans le réseau interne. Dans une telle situation, l'application devra être compatible avec un tel dispositif.

• Confidentialité
<p>La sécurité applicative, qui régit l'accès aux données selon le profil de l'utilisateur, doit faire l'objet de deux paragraphes distincts dans le cahier des charges :</p> <ul style="list-style-type: none">▪ un premier paragraphe qui précise dans un tableau la typologie et le nombre des utilisateurs▪ un deuxième paragraphe qui décrit pour chaque profil, de manière explicite, les cloisonnements et droits d'accès sur les données, en création, en mise à jour, en consultation. <p>Le principe du « besoin d'en connaître » doit être appliqué de manière à limiter l'accès aux seules informations explicitement autorisées.</p>

• Traçabilité
La traçabilité des accès et des tentatives d'accès à l'application ainsi qu'aux éléments considérés doit reposer sur un mécanisme de journalisation de l'activité des utilisateurs permettant de pouvoir les exploiter à posteriori.

Diffusion	Type	Référence	Page
Confidentiel	Instruction	F06-I6-rév5	12/12

Direction du Système d'Information

• Architecture applicative

La requête d'accès à l'application doit se faire auprès d'un service tiers et non via une interrogation directe de la base de données depuis le poste client.

L'ouverture de l'application à des utilisateurs extérieurs (hors réseau IFPEN) est conditionnée par l'utilisation d'un reverse proxy (qui sera situé en DMZ) et qui protégera les données et les autres composants de l'application situés dans le réseau interne.

Dans le cas où l'application nécessite des accès vers des sites externes, les flux doivent pouvoir transiter au travers d'un proxy

• Sécurité du développement

Limiter les fuites d'information techniques sur les logiciels utilisés par l'application.

Améliorer la prise en compte de la sécurité dans les développements Web particulièrement exposés.

Calculer les empreintes de mots de passe de manière sécurisée (i.e. permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute).

Réduire l'adhérence des applications à des produits ou technologies spécifiques.

• Accès externe au système d'information par un prestataire

Un accès externe pourra être envisagé en concertation avec le chef de projet IFPEN, des engagements contractuels spécifiques devront alors être prévus quant à l'utilisation de ce dispositif dans le contexte de la prestation.

La solution d'accès externe s'appuiera sur les infrastructures IFPEN, elle est basée sur une solution VPN SSL. Elle est mise à disposition et contrôlée par IFPEN : les solutions proposées par le prestataire ou externes ne sont pas autorisées.

Voici les engagements de sécurité associés auxquels doivent s'engager le prestataire :

- A ne se connecter qu'à partir de leur login propre (chaque login sera nominatif et ne devra être utilisé que par une seule personne), la liste des personnes susceptibles de se connecter devra être communiquée préalablement à IFPEN et mis à jour chaque fois que cela sera nécessaire.
- A se connecter qu'à partir d'adresses dûment identifiées et communiquées préalablement à IFPEN
- A n'intervenir que dans le seul but d'assurer la prestation du service pour lequel le prestataire a été sollicité
- A ne pas accéder ou tenter d'accéder à des postes ou équipements IFPEN autres que ceux mis à disposition à partir du portail d'accès.