FRANCE

Référence : IT_EFR_001_V13_FR_PRINCIPES DE SECURITE

EQUANS France - Direction des Systèmes d'Information

Principes de Sécurité

Applicable depuis le 15/04/2024

	REDACTEUR	VERIFICATEUR	APPROBATEUR	DIFFUSION
Fonction	Assistant RSSI	M-BISO BU France / L-CISO BU France	M-CISO BU FRANCE	A destination de EQUANS France et de ses entités
Nom	Equipe CYBER	Jérôme ARHUIS Ronan LAGATHU Guillaume VACHER	Suvansh LAL	

OBJECTIF : Ce document précise les modalités de mise en œuvre chez EQUANS France et ses entités des principes de sécurité et de résilience tirés des politiques de sécurité du Groupe EQUANS.

PERIMETRE D'APPLICATION : Les principes énoncés dans ce document s'appliquent à l'ensemble des départements, métiers et entités d'EQUANS France.

Indice	Date	Mises à jour apportées
01	21/03/2025	Création
10	18/04/2024	Approbation
11	31/03/2025	Intégration SI Client
12	16/04/2025	Validation de la version 13

Politique Groupe –

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

TABLE DES MATIÈRES

1. INTRODUCTION ET PRINCIPES GÉNÉRAUX 4

A. Définitions générales 4

B. Préambule 4

C. Corpus documentaires 4

D. Diffusion du document 5

E. Domaine d'application 5

PRINCIPES DE SECURITE 7

2. PRINCIPES COMMUNS 7

A. Organisation 7

B. Exigences légales, réglementaires et contractuelles 8

C. Sécurité de l'information dans les relations avec les fournisseurs 8

D. Gestion des risques 8

E. Classification et protection des données 9

F. Mesures de sécurité applicables aux personnes 10

3. SECURITE DES SI CORPORATE IT 12

A. Gestion des actifs 12

B. Contrôle d'accès 12

C. Gestion des identités 12

D. Authentification 13

E. Sécurité de l'information dans l'utilisation de services en nuage 14

F. Gestion des incidents 14

G. Continuité d'activité 15

H. Gestion de crise cybersécurité 16

I. Mesures de sécurité physiques 16

J. Équipements Utilisateurs 16

K. Gestion des vulnérabilités 17

L. Sauvegarde 17

M. Sécurité réseau 17

N. Cycle de vie de développement sécurisé 18

O. Gestion des changements 18

DOCUMENT PUBLIC. Tous droits réservés

Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

4. SECURITE DES SI CLIENT IT 19
A. Principes de sécurité applicables aux SI CLIENT IT 19
B. Gestion des Incidents et crises 19
C. Règlement Général pour la Protection des Données personnelles (RGPD) 20
TERMINOLOGIE 20

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

1. INTRODUCTION ET PRINCIPES GÉNÉRAUX

A. Définitions générales

Les définitions données ci-dessous s'appliquent à l'ensemble de ce document :

- **Entreprise** : EQUANS France ;
- **Groupe** : Groupe EQUANS ;
- **Utilisateur** : Toute personne (salarié, alternant, stagiaire, intérimaire, prestataire), quel que soit son lieu d'accès, disposant d'un compte lui donnant l'accès au Système d'Information (SI) de l'Entreprise ;
- **Client** : Entité externe ayant une relation contractuelle avec Equans ou une de ses entités affiliées pour laquelle sont exécutées des prestations. Celles-ci utilisent des produits ou services digitaux en support des activités réalisés par les collaborateurs d'Equans, entités affiliées et/ou leurs sous-traitants.
- **CORPORATE IT** : Ensemble des moyens informatiques et de télécommunications, matériels ou logiciels, que l'Entreprise met à disposition des Utilisateurs à des fins professionnelles ;
- **CLIENT IT** : Ensemble des moyens informatiques et industriels, matériels ou logiciels, mis à disposition par l'Entreprise ou le Client, que les métiers du Groupe utilise dans le cadre des activités d'intégration, maintenance, exploitation, supervision, développement.

B. Préambule

Dans un contexte général d'évolution des **menaces cybersécurité** et du renforcement du **cadre légal et règlementaire** (par ex. la Loi de Programmation Militaire, la Directive Nationale Sécurité, le RGPD, le Cyber Resilence Act, les Directives Européennes…), l'Entreprise est partie prenante dans la Sécurité du Système d'Information CORPORATE IT et de l'encadrement du niveau de sécurité des Systèmes d'Information CLIENT IT, sous la gouvernance du M-CISO France.

Ce document présente les **principes de sécurité** de l'Entreprise qui permettent d'atteindre ses objectifs sur les Sécurité du Système d'Information CORPORATE IT et CLIENT IT :

- respect des obligations légales et réglementaires ;
- devoir de conseil ;
- audit interne ;
- protection de ses infrastructures (SI) et de ses services applicatifs ;
- protection de ses données et celles de ses clients.

Ces principes s'appuient sur les exigences contenues dans les **politiques de sécurité du Groupe**, accompagnées des **mesures spécifiques** contextualisées par activité métier.

C. Corpus documentaires

- **Lettre d'engagement de la Direction Générale** : positionne l'importance de la sécurité de l'information au sein de l'Entreprise.
- **PSSI CORPORATE IT** : Politique de Sécurité du Système d'Information : contient les principes généraux en matière de sécurité du SI, les responsabilités et l'organisation, dont les mesures de sécurité techniques sont applicables au SI CORPORATE IT

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

- **PSSI CLIENT IT** : Politique de Sécurité du Système d'Information : contient les principes généraux en matière de sécurité du SI du groupe et gouvernance spécifique adaptée au contexte client, dont les mesures de sécurité techniques et organisationnelles sont applicables au SI CLIENT IT dédié à une affaire et sous contrat.
- **PSSI-O CLIENT IT** : Politique de Sécurité regroupant les mesures techniques et organisationnelles par domaine d'activité ou domaine technique. Elles sont le reflet des bonnes pratiques de l'ANSSI et/ou de normes tels que l'ISO 27002 :2022 ou l'IEC 62443.
- **Principes de sécurité** (ce document) : s'appuie sur la norme ISO 27002 :2022, présente de manière synthétique les mesures de sécurité en place, avec les références documentaires pour obtenir les détails de mise en œuvre (politique de domaine du Groupe, politique ou procédure spécifique à l'Entreprise…)
- **Politiques et procédures spécifiques** : ces documents viennent apporter des mesures qui sont spécifiques à l'Entreprise par rapport aux politiques de domaine du Groupe. Les mesures doivent être conformes à celles du Groupe. Il se peut par exemple qu'une contrainte légale ou réglementaire, spécifique à la France, vienne renforcer une mesure de sécurité du Groupe. Elles sont classées en deux catégories, COPORATE IT à destination Interne et CLIENT IT : contextualisées aux activités réalisées par les métiers du Groupe au bénéfice de leur Client.
- **Chartes** : charte d'utilisation des ressources informatiques de l'Entreprise, charte de l'administrateur, intégrées au règlement intérieur des sociétés juridiques du Groupe.
- **Les 10 Règles d'or de la Cyber** : 10 bonnes pratiques en matière de cybersécurité.
- **Déclaration d'Applicabilité (DdA) :** mesures de sécurité de l'Annexe A de la norme ISO 27001 :2022 avec, pour celles qui sont retenues, les références documentaires pour leur mise en œuvre.

Les documents concernant l'Entreprise sont disponibles sur l'Intranet « Ref'IT »[1]. Les documents concernant le Groupe sont disponibles sur l'Intranet « GRC EQUANS – Cybersecurity »[2].

D. Diffusion du document

Ce document est accessible à tous les Utilisateurs de l'Entreprise et de ses entités, en ligne sur l'Intranet. De plus, il est destiné à **être diffusé à l'extérieur de l'Entreprise**, par exemple pour accompagner une réponse à un appel d'offre ou un contrat.

Les autres documents du corpus documentaire de la Sécurité du SI de l'Entreprise et du Groupe n'ont **pas vocation à être diffusés largement.** Ils peuvent être consultés sur site, voire fournis à des auditeurs, avec l'**accord préalable du RSSI** de l'Entreprise.

E. Domaine d'application

Ce document a pour but de présenter la gouvernance CYBER unifiée d'Equans France.

Il est constitué en synthèse :

- des SI, qu'ils soient ou non hébergés par un tiers ;
- des Usagers des SI (collaborateurs, tiers externes …)

[1] https://equans.sharepoint.com/sites/DSIEQUANSFrance -> Sécurité S.I. [2] https://equans.sharepoint.com/sites/EQUANS-CyberSecurity

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

- des entités et BU attachées à l'Entreprise : ce sont les **Directions Générales** et les **lignes managériales** de l'Entreprise et des entités qui lui sont attachées qui portent la responsabilité de la mise en œuvre des exigences de sécurité.

Il est de **la responsabilité de l'Entreprise de veiller à la mise en œuvre des exigences de sécurité**, quand bien même leur déploiement opérationnel serait à la main d'un tiers (dans le cas d'un hébergement dans le Cloud, par exemple).

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

PRINCIPES DE SECURITE

2. PRINCIPES COMMUNS

A. Organisation

Le COMEX d'Equans France a désigné la Direction des Systèmes d'Information et son Département Cybersécurité en charge de l'application de la stratégie CYBERSECURITE du Groupe. Dans ce cadre la sécurité des systèmes d'information CORPORATE IT et CLIENT IT sont placés sous la gouvernance mis en place par le **M-CISO (RSSI) d'Equans France.**

Le Département Cybersécurité de la Direction des Systèmes d'Information d'Equans France est organisé comme en 5 pôles :

- GOVERNANCE RISK COMPLIANCE – Gestion des risques, conformité aux procédures et politiques
- SECURITY OPERATIONS – Suivi des vulnérabilités techniques et remédiations
- SECURITY PROJECT OFFICE – Gestion de l'intégration de la sécurité dans les projets
- DIGITAL RESILIENCY – Gestion de la résilience opérationnelle du CORPORATE IT
- CYBER CUSTOMER TRUST – Gestion des risques, Audit et Conseil sur les SI CLIENT IT

Ils s'appuient sur les Département Cybersécurité d'Equans CORP

- CYBER TECHNICAL OFFICE – Organe de gouvernance du Groupe Equans
- SLS CYBERDEFENSE – Centre de service SOC/CERT/CSIRT
- SLS CYBER CUSTOMER TRUST – Centre de service CCT

Les Départements de la DSI **déploient les mesures** de sécurité de leur périmètre, ils soutiennent et assistent le département Cybersécurité sur le SI CORPORATE IT.

Les Divisions métiers d'Equans France organisent les opérations métier au bénéfice de leur Client. Elles s'assurent de la cohérence des réponses opérationnelles terrain réalisées par les entités juridique qui portent les contrats. Dans ce cadre, elles peuvent être amenées à réaliser des activités d'intégration, maintenance, exploitation, supervision, développement au bénéfice de leur Client. L'encadrement du niveau de sécurité sur les SI CLIENT **est pilotée par le M-BISO d'Equans France** via le programme CYBER CUSTOMER TRUST FRANCE.

Les Usagers du SI CORPORATE de l'Entreprise **respectent les exigences** de la PSSI CORPORATE IT et de la Charte d'utilisation des ressources informatiques.

Les Usagers des SI CLIENT respectent les exigences propres à leurs contextes d'affaire. Dans ce cadre, les exigences Cybersécurité à prendre en compte sont explicitement mentionnées dans le contrat de l'affaire, en tant que clauses contractuelles et/ou Plan d'Assurance Sécurité. Elles peuvent être déclinées, si nécessaires au sein d'une PSSI CLIENT IT.

Le Programme CYBER CUSTOMER TRUST FRANCE est chargé d'encadrer le niveau de risque Cybersécurité en agissant en tant qu'audit interne et/ou conseil, au près des Divisions d'Equans France.

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

Les Clients sont invités, si besoin, à contacter leur **interlocuteur commercial ou opérationnel** qui relaie leur demande au département Cybersécurité de l'Entreprise.

B. Exigences légales, réglementaires et contractuelles

Comme le précisent les PSSI de l'Entreprise et du Groupe, les entités doivent se conformer aux **lois, règlements et engagements contractuels** les concernant.

Dans le cadre des activités d'Equans France, L'ensemble des exigences cybersécurité à intégrer dans le socle de conformité contractuel devra prendre en compte les particularités des réglementations relatives.

- aux Tiers (Ministère, Secteur Publique, Tertiaire, Privé …)
- aux typologies d'activité (Sûreté, systèmes embarqués, gestion des télécommunications …)
- aux lieux de réalisation des prestations par les métiers d'Equans France (Espace publique, ERP, IGH, espace réglementés, etc.)

La Direction Juridique et le Programme CYBER CUSTOMER TRUST mutualisent leurs compétences afin d'encadrer contractuellement ces points.

Pour des autres **périmètres spécifiques**, tels que des contrats pour l'industrie de la Défense où des données avec les mentions « Diffusion Restreinte » voire « Secret » sont manipulées, ou encore pour des activités menées hors du territoire français, **des mesures plus restrictives prévalent** dans ce cas sur celles de ce document et du corpus documentaire de politique de sécurité de l'Entreprise.

C. Sécurité de l'information dans les relations avec les fournisseurs

Dans les cas où l'Entreprise fait appel au service d'un tiers, les modalités de mise en pratique des principes et des règles de sécurité applicables doivent faire l'objet d'un document spécifique : **Plan d'Assurance Sécurité (PAS),** ou équivalent, corédigé et annexé au contrat.

Le document utilisé diffère selon la nature du service fourni :

- concernant les tiers mainteneurs ou les prestataires intervenant sur le SI de l'Entreprise, le PAS (ou équivalent) doit être fourni par le tiers, l'Entreprise **l'amende et/ou le valide** ;
- lorsqu'il s'agit de services SaaS confiés à des tiers, le **PAS** basé sur le modèle du Groupe est alors utilisé.

Les clauses de ce document sont proportionnelles et **adaptées aux activités** sous traitées dans ces accords (confidentialité, responsabilités, niveaux de service DICT, audits…)

Le cas échéant, le contrat porte une **clause de conformité** aux réglementations applicables (par exemple Secret de la Défense, RGPD, sectorielle…)

D. Gestion des risques[2]

Le M-CISO d'Equans France définit et maintien le **cadre de gestion des risques d'Equans France**.

Au sein des Systèmes d'Information CORPORATE IT, les analyses de risques :

- sont intégrées dans la gestion des projets ;
- s'appuient sur une méthodologie normalisée : EBIOS RM ;
- sont validées par le RSSI, revues lors d'évolutions majeurs ;

[2] Politique Groupe : EGP – Risk Management
Espace SharePoint « Sécurité dans les projets »

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

- utilisent les BIA en entrée ;
- fournissent les risques, avec leur probabilité et leur impact, selon les matrices présentes dans la politique de gestion des risques du Groupe.

Les risques critiques ou élevés doivent être traités pour que **leur niveau devienne acceptable**. Ainsi, un **plan de traitement des risques** est construit et revu régulièrement.

Au sein des Systèmes d'Information CLIENT IT, les analyses de risques sont obligatoires pour toute affaire dite sensible et ayant un impact significatif pour Equans France. Le programme CYBER CUSTOMER TRUST FRANCE garantira pour ces affaires :

- l'appréciation du niveau de risques en amont de la soumission de la réponse ;
- le suivi du niveau de risque tout au long de la vie de l'affaire ;
- s'appuie sur la méthodologie EBIOS RM par défaut ;
- sont validées par le COMITE RISQUES d'Equans France et/ou par la Direction Générale des Division métier.
- utilisent les BIA en entrée ;
- fournissent les risques, avec leur probabilité et leur impact, selon les matrices présentes dans la politique de gestion des risques du Groupe.

E. Classification et protection des données

L'Entreprise identifie 4 **niveaux de confidentialité** des informations : **Publique [TLP : WHITE], Interne [TLP : GREEN] niveau par défaut**, **Restreint [TLP : AMBER / AMBER-STRICT]**, **Secret [TLP : RED]**. Ces niveaux sont basés sur les besoins des métiers en matière de partage ou de restriction d'informations. Tous les actifs informationnels disposent d'un propriétaire et disposent d'une étiquette de classification.

Les propriétaires des données :

- fixent le bon niveau de classification ;
- veillent à ce qu'opérationnellement, les composants du SI concernés assurent les niveaux de **DICT** adaptés ;
- établissent les habilitations adéquates pour accéder aux informations (d'après les principes de moindre privilège et du besoin d'en connaître) ;
- donnent les exigences en matière de continuité d'activité.

L'Entreprise ne partage d'information confidentielle qu'en la présence d'un accord contractuel avec une clause de confidentialité ou avec un accord de non-divulgation (Non-Disclosure Agreement, **NDA**).

Tout Utilisateur, constatant ou suspectant un **incident** portant sur les données, contacte immédiatement son supérieur hiérarchique qui remonte directement l'information à la DSI.

Règlement Général sur la Protection des Données (RGPD) :

Le **DPO** de l'Entreprise veille au respect de la conformité au RGPD. Il s'appuie sur le registre des activités de traitement (article 30 du RGPD), tenu à jour grâce aux informations fournies par les propriétaires des données. Conformément aux recommandations de la CNIL, l'Entreprise procède à une Analyse d'Impact

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

relative à la Protection des Données (**AIPD**) lorsque « le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

La Charte d'utilisation des ressources informatiques précise les obligations des Utilisateurs en ce qui concerne le traitement des Données à Caractère Personnel (**DCP**).

Informations relevant de la Protection du secret de la Défense Nationale :

Le traitement de ces informations est sous gouvernance des Officiers de Sécurité et des Officiers de sécurité des SI des entités juridiques d'Equans France. Le SI CORPORATE IT n'est pas habilité à stocker les informations relevant des réglementations suivantes (IGI 1300, IM900, II901).

F. Mesures de sécurité applicables aux personnes

Dans le cadre d'une embauche, les équipes de recrutement de l'Entreprise effectuent des **vérifications de sécurité proportionnées** aux exigences métiers afin que le candidat puisse collaborer pleinement, par exemple en cas de besoin d'habilitation au « Secret de la Défense ».

Tous les Utilisateurs de l'Entreprise doivent confirmer avoir pris connaissance de la **Charte d'utilisation des ressources informatiques**, précisant les modalités d'usage du SI et des ressources mises à leur disposition (incluant la gestion de la confidentialité des données). La charte est diffusée et accessible à tous les Utilisateurs dès leur arrivée. Elle est annexée aux **règlements intérieurs des entités** précisant les sanctions encourues.

L'Entreprise **sensibilise** ses Utilisateurs à la sécurité du SI (risques, scénarios, bonnes pratiques…) avec la mise à disposition de supports adaptés, d'e-Learning et lors d'évènements spécifiques (sensibilisation au phishing, formation à la cybersécurité de groupes d'utilisateurs, intervention lors de séminaires métiers…).

Le **télétravail** est autorisé sous les conditions suivantes :

- les missions du collaborateur tolèrent le télétravail ;
- la demande du collaborateur a été validée par sa hiérarchie ;
- le collaborateur s'engage à utiliser uniquement les équipements (PC, smartphone, tablette…) fournis par l'Entreprise dans le cadre de son activité professionnelle.

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

3. SECURITE DES SI CORPORATE IT

A. Gestion des actifs

Les Ressources informatiques de l'Entreprise sont inventoriées au sein d'une **CMDB**. Une procédure détaille les attributs collectés et inscrits dans ce référentiel. On y trouve au minimum des informations sur le propriétaire de l'actif, son niveau de criticité et sa classification. La CMDB est **mise à jour** pour suivre les évolutions des actifs (par exemple une montée de version du système d'exploitation) ainsi que lors de leur retrait.

Des procédures encadrent le cycle de vie des actifs :

- Lors de la mise en place d'un nouvel actif, sa configuration respecte les directives de durcissement, selon le principe du « **security by design** ».
- Les processus de Maintien en Condition Opérationnelle (**MCO**) et de Maintien en Condition de Sécurité (**MCS**) sont détaillés dans des procédures spécifiques, par type d'actif.
- Des outils de **surveillance** remontent les dysfonctionnements et les événements de sécurité issus des atifs.
- Le décommissionnement / le recyclage / la **suppression d'un actif** se fait en accord avec les principes de sécurité, les réglementations et les besoins métiers : délai de conservation des données, preuve de destruction, procédures de destruction des supports de stockage…

B. Contrôle d'accès

Tout Usager doit être authentifié dès lors qu'il accède à au SI de l'Entreprise, en conformité avec les **habilitations** dont il dispose.

L'Entreprise **trace les accès** de tous les Utilisateurs au SI et les actions les plus sensibles.

Les demandes d'habilitation aux applications respectent les bonnes pratiques et en particulier :

- les **demandes** sont tracées dans les outils de gestion des tickets ;
- les accès sont accordés selon les principes du '**moindre privilège**' et de la '**séparation des tâches**' ;
- les **rôles** sont attribués par profils métier.

L'Entreprise réalise régulièrement des **revues d'habilitations** dont la fréquence est adaptée à la sensibilité des accès. Les accès privilégiés au SI des administrateurs sont renforcés : complexité des mots de passe adaptée, authentification multi-facteurs (MFA) spécifique, charte administrateur, protocoles sécurisés, clés physiques, bastion…

Les accès au SI de l'Entreprise depuis l'extérieur (télétravail, tierce maintenance applicative…) s'appuient sur l'utilisation d'une solution de type 'Zero Trust' avec MFA.

C. Gestion des identités[3]

La gestion des identités au sein du Groupe et de ses entités s'appuie sur le 'Group Identifier' (GID) : identifiant alphanumérique unique, qui permet d'identifier un Utilisateur au sein **du référentiel des**

[3] Politique Groupe: EGP – Identity Management and GID

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

identités du Groupe. Tout personne qui accède au SI CORPORATE IT du Groupe doit disposer d'un GID, en excluant les 'invités Office 365'.

L'allocation d'un GID doit se faire via la solution du Groupe, en fournissant des informations permettant d'**identifier de façon unique** l'Utilisateur. Même après un départ du Groupe, un GID n'est jamais réutilisé pour une personne différente. Une personne conserve sont GID même si son statut change (suite à une internalisation par exemple).

Tous les accès aux solutions techniques et aux applications métier des entités doivent **s'appuyer sur le GID** au travers de l'annuaire Groupe.

Il est du ressort des Ressources Humaines et de la ligne managériale de l'Entreprise et de ses entités de gérer le **cycle de vie des identifiants** en :

- **anticipant** les arrivées, départs et mobilités des personnes (internes comme externes) ;
- **réalisant une vérification** chaque année, pour les externes dont la durée de l'engagement dépasse 12 mois, avant de renouveler les droits ;
- **déclarant** dès que possible une fin de contrat/mission et en s'assurant qu'elle soit effective dans le SI la semaine suivant la date de fin.

La procédure de **désactivation en urgence** d'un compte peut être déclenchée sur demande des Ressources Humaines ou par le CERT (en cas de compromission). Celle-ci garantit une suppression de l'intégralité des droits d'accès en moins de 24 heures.

Les comptes personnels d'**administration** doivent s'appuyer sur des identifiants **spécifiques**, distincts des comptes personnels standards. Les règles d'authentification pour ces comptes sont renforcées (cf. section suivante). Les devoirs et les usages sont précisés dans la Charte de l'administrateur. Les administrateurs disposant de privilèges élevés et globaux (administrateurs de domaine, etc…) signent un engagement.

D. Authentification[4]

Les Usagers du SI CORPORATE de l'Entreprise s'engagent à respecter les directives présentes dans la **Charte d'utilisation des ressources informatiques**, en particulier :

- garder secrètes les informations d'authentification ;
- respecter les règles de complexité de mot de passe ;
- utiliser des informations d'authentification différentes entre les usages professionnels et personnels ;
- utiliser un compte personnel d'administration, pour les tâches d'administration du système, qui diffère du compte d'utilisation standard.

Les mots de passe sont **chiffrés** en transit et dans les bases où ils sont stockés.

Les accès au SI s'appuient obligatoirement sur l'utilisation de mécanismes **SSO** et **MFA**. L'authentification via SSO est basée sur la fédération des identités du Groupe, afin d'associer l'ensemble de leurs accès à leur compte principal. Cette pratique concerne toutes les applications, y compris celles en SaaS.

[4] : EGP Authentication & Password

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

E. Sécurité de l'information dans l'utilisation de services en nuage[5]

Les principes énoncés ci-dessous sont spécifiques au périmètre du SI hébergé au sein de Fournisseurs de Services Cloud (**FSC**). Tous les principes des autres thématiques sont aussi à respecter dans les espaces Cloud de l'Entreprise (par exemple la gestion des vulnérabilités, le contrôle des accès, etc.)

Les espaces Cloud de l'Entreprise sont organisés dans une structure en arborescence dont le niveau « racine » est géré par le Groupe. Au sein de ces espaces, la gestion des comptes, des ressources et des projets est alignée avec les **directives du Groupe** (propriétaires identifiés, revues régulières des comptes, authentification sécurisée, ISP…)

Les règles de filtrage au niveau du réseau et sur les serveurs sont aussi fines que possible. L'Entreprise s'appuie sur l'outil de gestion des adresses IP (**IPAM**) du Groupe. Les connexions au cœur de réseau du Groupe sont soumises à des exigences spécifiques. L'exposition des actifs à Internet s'appuie sur des solutions de sécurité : firewall, **WAF** (Web Application Firewall, pare-feu applicatif Web), répartiteurs de charge, solution anti DDoS, des protocoles de chiffrement « à l'état de l'art » …

Les Ressources informatiques hébergées chez les FSC sont supervisées par des outils Groupe du type Cloud-Native Application Protection Platforms (**CNAPP**) et font l'objet d'indicateurs de suivi.

F. Gestion des incidents[6]

L'Entreprise dispose d'un processus de **journalisation** pour collecter et protéger toute information permettant la détection d'un **événement de sécurité** ou la conduite d'une enquête à la suite d'un **incident de sécurité** avéré. La rétention des informations collectées est proportionnée et en accord avec les règlementations en vigueur.

Un processus de cybersurveillance s'appuie sur ces informations pour déclencher des alertes émises au GSOC (Group Security Operational Center), qui fait partie du **CSIRT**.

Contributeurs et rôles :

Fonction	Missions
Utilisateurs	Signalement des incidents de sécurité (avérés ou suspectés) au département cybersécurité de la DSI
Département cybersécurité de la DSI	Suivi des incidents et crises cybersécurité
Les autres départements de la DSI	Gestion d'incident
RSSI et un membre de la Direction	Déclenchement du processus de crise
CSIRT / GSOC (SLS Cyber Défense)	Suivi en temps réel des alertes sur les actifs (postes, réseaux, applications…) et réponse à incident
CERT (SLS Cyber Défense)	Pilotage de la gestion de crise au niveau du Groupe

[5] : EGP Cloud Security Policy
[6] : EGP Security Incident Response Policy

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

Une fois l'incident de sécurité qualifié, des mesures d'urgence peuvent être prises, afin de **limiter les impacts** et de préserver les traces. En parallèle du confinement, une **investigation** est lancée afin d'identifier les caractéristiques de l'incident.

Les incidents de sécurité ayant déclenché une gestion de crise cyber sont tracés et font l'objet d'un plan d'action de correction suivi par le RSSI de l'Entreprise.

G. Continuité d'activité

Sur la base des besoins des métiers en matière de disponibilité, l'Entreprise a défini des Plans de Continuité d'Activité (**PCA**) pour permettre le **maintien des activités** métiers malgré la survenance d'incidents rendant tout ou une partie du SI indisponible.

Le processus de PCA est détaillé dans un document qui définit :

- les conditions de déclenchement du plan (y compris auprès de tiers) ;
- les conditions de reprise normale des activités ;
- les rôles et responsabilités des acteurs du plan ;
- la documentation nécessaire ;
- les modalités de communication durant le plan ;
- les modalités de contrôle du bon fonctionnement du plan.

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

Le processus est **mis à jour** au besoin, pour prendre en compte les évolutions du SI qui l'impactent (par exemple un changement de fournisseur pour des applications en SaaS, un remplacement d'équipements réseau, une évolution dans l'infrastructure, etc.)

Le PCA est **régulièrement testé** par des exercices de continuité d'activité.

Parmi les PCA, on distingue :

- les Plans de Continuité Opérationnelle : dont les Métiers sont propriétaires et responsables ;
- les Plans de Continuité Informatique : à la charge de la DSI.

H. Gestion de crise cybersécurité[7]

Un incident cybersécurité présentant des caractéristiques particulières (notamment d'impact et / ou d'absence de maîtrise) déclenche le **processus de crise**, qui inclut :

- les conditions d'entrée en crise ;
- les conditions de sortie de crise ;
- les rôles et responsabilités des acteurs identifiés à chaque étape ;
- la mobilisation des cellules de crise (technique, opérationnelle, décisionnelle) ;
- les moyens au service de la gestion de crise ;
- les modalités d'information de la gouvernance de la sécurité de l'information ;
- les modalités de reporting associées au dispositif de pilotage de la sécurité de l'information.

Le processus de gestion de crise fait l'objet **d'exercices réguliers**.

I. Mesures de sécurité physiques

Les sites d'hébergement Cloud du SI utilisés par l'Entreprise sont à **accès restreint** et font l'objet d'un contrôle strict (ex : accès par badge habilité…). Les sites sont certifiés ISO 27001 et respectent l'état de l'art du marché sur la sécurité physique (au minimum Tier III).

L'accès d'un grand nombre de locaux ou de bureaux de l'Entreprise est sécurisé par l'emploi de **badges nominatifs**. Tout visiteur doit être accompagné, de son entrée jusqu'à sa sortie du bâtiment, par une personne interne à l'Entreprise.

J. Équipements Utilisateurs

La **Charte d'utilisation des ressources informatiques** fournit les règles d'utilisation des postes de travail et des équipements mobiles.

L'utilisation des postes de travail se fait par un compte personnel standard, qui ne dispose pas des droits d'administration. Seuls les logiciels validés par la DSI peuvent être installés sur les postes de travail. Les actions d'administration, telles que l'installation d'un logiciel, se font au travers d'un processus qui nécessite une validation managériale et/ou de l'équipe sécurité.

Des **logiciels de sécurité** protègent et analysent les postes de travail (antivirus comportemental, accès distant de type « zero trust », filtrage Internet permanent, firewall…).

[7] Politique EQUANS France: Plan de Gestion de crise Cyber [10:]
EGP Information Systems Security Policy

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

L'Entreprise ne permet pas l'utilisation de BYOD (Bring Your Own Device) : l'utilisation d'un équipement mobile personnel à des fins professionnelles. Elle fournit à certains Utilisateurs des tablettes et/ou smartphones. Ces équipements sont suivis au travers d'un outil de gestion centralisée.

Tout vol ou perte d'un équipement informatique professionnel doit faire l'objet d'une déclaration auprès des autorités compétentes (services de police, gendarmerie, etc.) et auprès du service informatique afin de procéder à la désactivation de l'équipement et si possible à la suppression des données.

K. Gestion des vulnérabilités[8]

Une **veille permanente** sur les vulnérabilités est menée par la SLS Cyber Défense avec l'équipe VMCT (Vulnerability Management and Compliance Team), au sein du CERT. Elle permet d'identifier les **failles** de sécurité et les **correctifs** associés applicables aux composants du SI, de façon à définir et mettre en œuvre des plans de réaction adaptés et proportionnés.

Des **scans de vulnérabilités** sont effectués au minimum une fois par semaine sur le SI de l'Entreprise.

Les scans s'appuient sur : l'inventaire des assets de l'Entreprise à scanner : issu de la **CMDB** (cf. section sur la gestion des actifs) et fourni au CERT ; les consignes (fréquence de scan, type de scan, etc.) contenues dans la procédure de scan du Groupe. L'Entreprise priorise le traitement des vulnérabilités en coordination avec le CERT. Lorsqu'il n'est pas possible de remédier à une vulnérabilité, une analyse de risques est menée (cf. section sur la gestion des risques) et des **mesures de mitigation** sont déployées pour abaisser le niveau de risque. Le CERT mène un suivi du **plan de remédiation** de l'Entreprise.

L. Sauvegarde[9]

Pour les actifs critiques, la règle de sauvegarde **« 3-2-1 »** est privilégiée (3 copies, 2 types de support, 1 copie hors site), accompagnée du chiffrement des sauvegardes.

Les besoins en matière de sauvegarde sont définis en coordination avec les métiers pour définir la durée maximale d'interruption (Recovery Time Objective, **RTO**) et la quantité maximum de données qu'il est acceptable de perdre (Recovery Point Objective, **RPO**).

Dans le cadre du Plan de Reprise après Sinistre (Disaster Recovery Plan, **DRP**), des **tests de sauvegarde** et de restauration sont régulièrement menés pour vérifier la capacité à respecter les besoins métiers.

Les sauvegardes sont supprimées lorsque le **délai maximum de conservation**, fixé selon les besoins métiers, est atteint. Des contrôles réguliers vérifient la bonne application de ce principe.

Les systèmes de sauvegarde sont surveillés, les journaux et pistes d'audit sont conservés. La bonne exécution des sauvegardes est vérifiée quotidiennement.

M. Sécurité réseau

L'Entreprise exploite une architecture **cloisonnée** avec un découpage en zones logiques en fonction des usages et notamment :

---

[8] : EGP Vulnerability Management

[9] : EGP Data Backup Management Policy

DOCUMENT PUBLIC. Tous droits réservés

Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

- une zone regroupant les serveurs qui hébergent des services ayant vocation à communiquer avec l'extérieur ;
- une zone privée regroupant les serveurs n'ayant pas vocation à communiquer avec l'extérieur.

Des dispositifs et des **règles de filtrage** sont implémentés pour définir l'accès aux différentes zones. Les échanges autorisés entre ces différentes zones sont définis en fonction de l'analyse de risques, ils sont filtrés, surveillés et contrôlés. Le filtrage respecte le principe selon lequel tout échange qui n'est **pas explicitement autorisé est interdit**. Chaque demande d'évolution de règle interzones fait l'objet d'une demande formalisée et tracée et d'une validation formelle de la filière sécurité.

Les flux vers ou depuis Internet sont filtrés et surveillés. Lorsqu'une application est exposée à Internet, elle est protégée par un **WAF** (Web Application Firewall, pare-feu applicatif Web) en mode blocage. L'utilisation de protocoles non sécurisés, non pris en charge ou en fin de vie est interdite.

N. Cycle de vie de développement sécurisé

Les applications développées par des Utilisateurs de l'Entreprise doivent répondre aux exigences de sécurité du Groupe.

Les **outils de développement** utilisés au sein de l'Entreprise sont sélectionnés par les équipes DSI qui veillent à l'application des mises à jour et des patchs de sécurité.

Pour le développement des applications, les équipes s'appuient sur les **bonnes pratiques**, issues des standards en termes de qualité de code, et celles qui sont spécifiques à l'Entreprise. Les standards en termes de sécurité sont aussi respectés (par exemple l'absence de mot de passe dans le code). Les projets sont documentés (Dossier d'Architecture Technique, schémas d'architecture, etc.).

Les codes sources sont stockés dans un **référentiel centralisé** ('repository') dont l'accès est sécurisé.

Des outils contrôlent la **qualité du code** et signalent des failles de sécurité. Le cycle de vie des bibliothèques de code externe est suivi par les équipes DSI et cybersécurité ; en cas de nécessité, une validation préalable par l'équipe cybersécurité peut être demandée avant implémentation.

O. Gestion des changements

Un processus de gestion des changements est en place au sein du Groupe et de l'Entreprise. Tous les changements sont journalisés dans un outil de ticket.

Les changements qui ont un **impact notable** sur le SI de l'Entreprise sont analysés au cours d'un **CAB** (Change Advisory Board : Comité de Validation des Changements), que ces changements soient initiés au niveau de l'Entreprise ou au niveau du Groupe.

Les éléments ci-dessous sont analysés :

- l'objectif / la raison du changement ;
- l'analyse d'impact ;
- la procédure de retour arrière ;
- le lotissement ;
- la gestion de la communication…

L'Entreprise distingue **plusieurs environnements** hors production (ex : développement, recette, préproduction) afin de sécuriser les mises en production et de minimiser l'indisponibilité des services.

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

4. SECURITE DES SI CLIENT IT

En préambule, les principes de l'organisation définis dans le paragraphe « 2. PRINCIPES COMMUNS » s'appliquent aux SI CLIENT et sont complétés par les points suivants :

A. Principes de sécurité applicables aux SI CLIENT IT

Le contrat et les éléments contractualisées prévalent sur les politiques groupe. Le CLIENT défini le niveau de sécurité attendu pour la prestation des métiers d'Equans France. Les exigences de sécurité doivent être transmises explicitement. Elles peuvent être formalisées sous forme de :

- Clauses contractuelles ;
- Plan d'Assurance Sécurité annexé au contrat ;
- Autres pièces contractualisées (FTM, Ordre de service…).

Les exigences de sécurité doivent être équilibrées vis-à-vis du droit applicable. CYBER CUSTOMER TRUST se tient au côté des métiers d'Equans France pour analyser précisément le socle de conformité et de règlementation de l'affaire en prenant en compte les exigences réglementaires applicables :

- aux tiers (CLIENT, SOUS-TRAITANT) ;
- aux activités réalisées par les métiers d'Equans France (Exploitation, Maintenance, Intégration…) ;
- aux domaines d'activités (Défense, Sécurité, Sûreté) ;
- aux lieux d'exécution de ces activités (Espace public, ERP, EGH…).

CYBER CUSTOMER TRUST peut être sollicité à chaque nouveau contrat ou pour tout renouvellement.

Pour toute question : cct.france@equans.com

B. Gestion des Incidents et crises

Le Département Cybersécurité d'Equans France apporte son support pour le domaine de la Cybersécurité aux Divisions métiers.

En cas de risque élevé, il peut faire appel au dispositif de FAST INCIDENT RESPONSE composé d'Internes d'Equans et de prestataire qualifiés PASSI par l'ANSSI.

En cas d'incident majeur, le CLIENT doit respecter la gouvernance de son affaire et solliciter son RESPONSABLE d'AFFAIRE qui escaladera aux équipes du Département CYBERSECURITE d'EQUANS France.

Pour toute question : cct.france@equans.com

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

C. Règlement Général pour la Protection des Données personnelles (RGPD)

Pour toute demande relative au RGPD ou pour tout exercice de droit, contacter : privacy.france@equans.com

TERMINOLOGIE

BIA – Business Impact Analysis :
Processus qui permet d'identifier et d'évaluer les impacts potentiels d'une interruption d'activité sur une entreprise.

CCT – Cyber Customer Trust :
Programme du groupe Equans visant à réduire l'exposition aux risques dits de « cybersécurité » des activités réalisées pour ses clients intégrant une composante Digitale. **CERT – Computer Emergency Response Team :**
Pour le Groupe, cette fonction est assurée par la SLS Cyber Défense. Le CERT a pour missions : le partage de connaissances (veille sécurité, sensibilisation et formations), l'évaluation des vulnérabilités et le pilotage de la gestion de crise.

CMDB – Configuration Management DataBase :
Base de données de gestion de configuration : référentiel qui sert d'entrepôt de données pour les installations IT. Il contient des données relatives à un ensemble des actifs IT, ainsi que des relations descriptives entre ces actifs**CNIL – Commission Nationale de l'Informatique et des Libertés :**
En France, la CNIL est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.

CSIRT – Computer Security Incident Response Team :
Pour le Groupe cette fonction est assurée par la SLS Cyber Défense. Le CSIRT a pour missions : la détection des événements de cyber sécurité, le triage et l'analyse de ces événements, l'investigation et la réponse à incident, gestion des menaces cyber.

DICT – Disponibilité, Intégrité, Confidentialité, Traçabilité :
(En anglais, CIAT : Confidentiality, Integrity, Availability, Traceability) caractéristiques que le propriétaire ou le gestionnaire de l'information veut voir réalisées afin de s'assurer que la sécurité est au rendez-vous pour ses données.

DPO – Data Protection Officer :
Délégué à la protection des données : personne en charge de la protection des données à caractère personnel traitées par un organisme (administration, entreprise...).

ISP – Intégration de la Sécurité dans les Projets :
C'est l'un des éléments fondamentaux de l'approche "security by design". Elle permet d'anticiper les besoins de sécurité et de protéger les entreprises contre les principaux risques qu'elles pourraient encourir dans le cadre de leurs activités numériques. Souvent associée à des référentiels ou des méthodologies basés sur l'approche des risques IT, l'ISP permet d'accompagner les projets au début, pendant et jusqu'à la fin de ces derniers.

DOCUMENT PUBLIC. Tous droits réservés
Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.

MFA – Multi Factor Authentication (Authentification Multi facteur) :

Méthode accordant l'accès uniquement si l'utilisateur présente deux facteurs d'authentification ou plus parmi ces types de facteur : ce que l'on connait (un mot de passe, un code PIN), ce que l'on a (un "hard token", un smartphone avec une application "soft token"...), ce que l'on est (biométrie telle qu'une empreinte digitale, une reconnaissance faciale...)

NDA – Non-Disclosure Agreement :

L'accord de non-divulgation est un contrat entre deux entités qui engage l'une de ces entités à tenir confidentielles certaines informations que l'autre sera amenée à lui communiquer. L'accord peut également être « mutuel », c'est-à-dire que l'une et l'autre des entités s'engagent à ne pas diffuser certaines informations échangées.

RGPD – Règlement Général sur la Protection des Données :

(Terme anglais : GDPR, General Data Protection Regulation) Règlement de l'Union Européenne qui constitue le texte de référence en matière de protection des Données à Caractère Personnel

RSSI – Responsable de la Sécurité des Systèmes d'Information :

(Terme anglais : CISO, Chief Information Security Officer) Définit et développe la politique de sécurité de l'information de son entreprise. Il est garant de sa mise en œuvre et en assure le suivi. Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte.

SaaS – Software as a Service :

'Logiciel en tant que service' : modèle de distribution de logiciel. Il permet à un fournisseur tiers d'héberger des applications et de les mettre à la disposition des clients via l'internet.

SI – Système d'Information :

Ensemble des processus, ressources organisationnelles, matérielles et logicielles de l'Entreprise permettant d'acquérir, de générer, de traiter, de stocker, de détruire, de diffuser, de transmettre ou d'accéder à des informations électroniques au sein de l'Entreprise.

SSO – Single Sign On :

Méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques (ou sites web sécurisés) en ne procédant qu'à une seule authentification.

VPN – Virtual Private Network :

Un réseau privé virtuel est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

DOCUMENT PUBLIC. Tous droits réservés

Les copies téléchargées ou papier de ce document ne sont pas maîtrisées. Vérifiez que la version de ce document est celle en vigueur.