VOLKSWAGEN FINANCIAL SERVICES

Référence	**Manuel de l'organisation (L-OHB) – Volkswagen Bank France**
Titre de la procédure	**PC Guideline France – Charte informatique**
Direction(s) concernée(s)	DSI
Date de validité	01/09/2020
Version remplacée	01/12/2016
Propriétaire	DSI (GRC)
Résumé	Cette procédure permet de définir et mettre en œuvre les moyens appropriés pour protéger les utilisateurs et les moyens informatiques mis à leur disposition contre les risques de destruction, d'altération, de fraude ou encore de vol. Elle présente également les obligations et les responsabilités des utilisateurs en matière de sécurité de l'information.
Classification	Interne

Table des matières

Validation

	Rédaction	Validation et approbation				
Nom	Gérald GREVREND	Martin SCHOLTER	Jérôme BEGORRE	Xavier DESTRUHAUT	Dirk PANS	Thierry VERBIST
Fonction	Chef de Service IT Gouvernance Risque et Conformité	Chef de DPT Juridique et Conformité	DSI	Directeur des Ressources Humaines et Services Généraux	Directeur de succursale Front-Office	Directeur de succursale Back-Office
Date		11/06/2019				
Signature						
Nature des modifications	• Alignement avec OMEB G07.G14 PC Guideline v2020.08 • Alignement avec IOHB G07.G14 PC Guideline v2020.08 • Clarification liée à GDPR • Mise à jour des contacts					

Visa du service Juridique (VW FS France)	
Date de revue	
Visa de GRM (VWFSAG)*	N/A
Date de revue	

** Conformément au MA Risk*

Registre des modifications

Date	Qui	Résumé
12/08/2020	Gérald Grévrend	Contacts, référence to RGPD and DPO
12/08/2020	Gérald Grévrend	Mise à jour des règles de mot de passe, sur l'utilisation des clients mobiles et le transport de données
12/08/2020	Gérald Grévrend	Création du registre de modifications

1. Contexte et objet de la procédure

Le présent document est rédigé dans l'intérêt de chacun des utilisateurs du système d'information (SI) de Volkswagen Bank France et manifeste la volonté de Volkswagen Bank France de :

- Respecter les lois et règlementations en vigueur, notamment pour le respect de la vie privée et du secret des correspondances visés par les articles 9 du Code Civil et 226-15 du Code Pénal,
- Assurer un développement harmonieux des accès au SI de Volkswagen Bank France pour les utilisateurs,
- Définir et mettre en œuvre les moyens appropriés, selon l'état de l'art de la technique, pour protéger les utilisateurs et les moyens informatiques mis à leur disposition contre les risques de destruction, d'altération, de fraude ou encore de vol.

Volkswagen Bank France est seul habilité à l'ouverture et au maintien des accès à son SI. Il fournit notamment à ses employés et à ses prestataires des moyens informatiques destinés à un usage professionnel. En vue de maintenir un environnement de travail professionnel et de protéger les informations confidentielles qui sont la propriété de Volkswagen Bank France, de ses clients ou encore de ses partenaires, chaque utilisateur est tenu de respecter un certain nombre de directives mentionnées dans le présent document.

Le présent document a pour objet de préciser les droits et devoirs des utilisateurs des SI. Il est conforme aux dispositions légales et règlementaires en vigueur. Il définit notamment les règles d'utilisation et d'accès :

- Aux systèmes d'information
- Aux services Internet,
- Aux ordinateurs de bureau, portables, serveurs,
- Au courrier électronique et autres outils d'échanges d'information,
- Aux services intranet et extranet
- A la téléphonie
- Et de manière générale à l'ensemble de l'infrastructure et des moyens informatiques

Selon la structure documentaire de l'OMEB et de IOHB, le document est classé comme suit :

- Type de document : Politique
- Document de niveau supérieur: Politique de Sécurité de l'Information
- Processus : G07 Manage Security

1.1 Qu'est-ce que la sécurité de l'information

L'information est un élément stratégique pour VW Bank France. C'est un outil de prise de décision de l'entreprise et peut être collectée, traitée, conservée ou communiquée au sein de l'organisation ou auprès de nos partenaires.
La sécurité de l'information consiste donc à protéger le patrimoine informationnel de VW Bank France contre les risques de destruction, d'altération, de fraude ou encore de vol.

1.2 Quelles informations protéger ?

Chaque employé (interne ou externe) ou tierce partie qui a un accès légitime aux systèmes d'information accède également aux informations de Volkswagen Bank France et participe activement aux mesures de sécurité.

La société définit trois types d'information nécessitant une protection :

- **Information secrète**: Information qui peut menacer la réalisation des objectifs de la Société durablement si elle obtenue par des personnes non autorisées. Elle doit donc être soumise à une liste de diffusion extrêmement restreinte et à des contrôles stricts.
- **Information confidentielle**: Information qui peut menacer la réalisation des objectifs de projets ou de production si elle est obtenue par des personnes non autorisées. Elle ne doit être accessible que par un cercle autorisée et limitée. Cette catégorie inclut également des données personnelles qui, dans le contexte, permettent des conclusions sur une personne physique (cf. § 7.2.7.9)
- **Information interne**: Information qui n'est pas destinée à une diffusion publique et qui ne doit être divulguée qu'au sein de Volkswagen Bank France. L'information de Volkswagen Bank France ne doit pas être diffusée à une tierce partie sauf si :
  - L'information est catégorisé comme publique
  - Le propriétaire de l'information approuve sa diffusion
  - Les parties externes sont dépendantes de l'information pour une mission de coopération.

1.3 Responsabilité de l'employé au regard de la sécurité de l'information

Chaque employé est tenu d'une obligation de confidentialité par son contrat de travail et chaque contractant est tenu d'une obligation de confidentialité par le contrat. Ils doivent s'assurer de l'application des règles de sécurité dans sa relation aux informations de l'entreprise ou aux systèmes de traitement de l'information.

Cela inclut :

- La prévention des accès non-autorisés
- La prévention de la compromission ou du vol des informations de l'entreprise ou des systèmes de traitement des informations
- La garantie de l'exactitude des contenus des données
- La garantie de la conformité avec les dispositions règlementaires et légales, particulièrement les règles locales de protection de données aussi bien commerciales que fiscales.
- La sauvegarde des droits et des intérêts des personnes physiques et morales qui maintiennent une relation d'affaires avec Volkswagen Bank France.

Les employés doivent participer aux formations proposées pour le bon usage et la sécurité des services informatiques.

Les employés et les contractants doivent se conformer à la politique de confidentialité des Données à Caractères Personnel de la société VW BANK.

Il est à noter que le présent document vient en ajout du Règlement Intérieur (RI), notamment de son article 19 du RI.

1.4 A quelle réglementation sécurité faudrait-il se conformer?

Des obligations de sécurité de l'information relevant de textes d'ordre législatif et réglementaire encadrent les employés dans leur travail quotidien. Elles décrivent en détail les exigences auxquelles doivent se conformer chaque utilisateur des services informatiques, en particulier en termes de règles sécurité et reposent sur les procédures suivantes :

- Politique de Sécurité des Systèmes d'Information
- Sécurité du Poste Client
- Sécurité des Clients mobiles
- Classification de l'information
- Data Protection Guideline

Il est à noter que toute infraction relative aux règlements de sécurité peut avoir des conséquences disciplinaires.

1.5 En cas d'incident de sécurité de l'information?

(Cf. § 7.2.5Assistance)

2. Diffusion

- Ensemble des personnes disposant d'un accès au SI interne de Volkswagen Bank France : salariés, stagiaires, intérimaires, apprentis, prestataires.

3. Domaine d'application

Ce document couvre l'ensemble des activités de Volkswagen Bank France et de ses filiales ou participations. Il couvre également les sous-traitants de Volkswagen Bank France.

Aux personnes internes Volkswagen Bank France

Toute personne interne qui signe un contrat de travail avec Volkswagen Bank France doit avoir pris connaissance de ce règlement. Il se trouve dans les annexes au dossier administratif relatif au contrat d'embauche fournis par le service des ressources humaines. Chaque collaborateur doit confirmer l'avoir lu et approuvé par écrit.

La preuve de confirmation écrite doit être conservée dans le dossier administratif de chaque salarié au Service des Ressources Humaines.

Prestataires ou Fournisseurs externes

Pour les personnes externes travaillant pour Volkswagen Bank France, ce règlement doit faire partie d'une série de documents annexés au contrat remis par le service des Achats Volkswagen Bank France, lors de la signature des marchés. Le Prestataire ou Fournisseur doit confirmer l'avoir lu et approuvé par écrit.
La preuve de confirmation écrite doit être conservée par le Service des Achats. Le Prestataire ou Fournisseur doit également en conserver une copie.

4. Références

4.1 Directives «Guidelines» Volkswagen Bank Group (OMEB)

- G07.P14 PC Guideline
- Data Protection Guideline
- Security Guideline for Mobile Clients
- Information Security Policy
- Information Security Classification and Handling Guideline

4.2 Directives «Guidelines» Volkswagen Financial Services AG (IOHB)

- G07.P14 PC Guideline
- Data Protection Guideline

- Security Guideline for Mobile Clients
- Information Security Policy
- Information Security Classification and Handling Guideline

4.3 Procédures Volkswagen Bank France

- Politique de Sécurité des Systèmes d'Information
- Règlement intérieur

4.4 Modes Opératoires

- Trucs et astuces (Cf. 9.2)

4.5 Lois et réglementations

- Code du travail
- Loi informatique et Libertés
- Code Civil
- RGPD
- Code pénal
- Loi du 31 mai 2019, appelé LIL 4

5. Affectation des rôles et des responsabilités

Responsabilité	Personne responsable / Département
Révision et mise en œuvre de cette procédure	IT GRC
Approbation des dérogations	IT GRC
Administration des périphériques	Administrateurs
Conformité avec la procédure des Mots de passe	Utilisateurs
Conformité avec la procédure de l'antivirus	Utilisateurs
Rapport des incidents de sécurité	Utilisateurs
Conformité avec les règlements sur la vie privée en public	Utilisateurs
Conformité au RGPD et validation des mesures prises	DPO (Juridique) / IT GRC (IT)

6. Définitions principales

- **Administrateur :** Un administrateur ou administrateur technique ou encore gestionnaire techniques est une personne en charge du maintien en conditions opérationnelles de tout ou partie du réseau informatique de Volkswagen Bank France dont les PC font partie.
- **CNIL :** La Commission nationale de l'informatique et des libertés est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle exerce ses missions conformément à la loi informatique et libertés qui la qualifie d'autorité administrative indépendante.
- **LISO :** Local Information Security Officier est le responsable de Volkswagen Bank France en matière de sécurité des systèmes d'information.

- **PC :** Personnal Computer ou ordinateur personnel. C'est un ordinateur destiné à l'usage d'une personne. Dans le cas présent, la notion de PC englobe l'ensemble des terminaux informatiques (notamment les serveurs, les stations fixes et les ordinateurs portables), y compris les appareils mobiles de type Smartphones et les supports amovibles (clés USB et disques durs externes) mis à la disposition par Volkswagen Bank France auprès de ses collaborateurs.
- **PSSI :** Politique de Sécurité du Système d'Information. Ceci regroupe l'ensemble de la documentation relative à la politique sécurité du SI de Volkswagen Bank France.
- **SI** : le Système d'information est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de collecter, regrouper, classifier, traiter et diffuser de l'information sur un environnement donné. Le SI est en partie constitué est moyens informatiques de l'entreprise.
- **Disponibilité :** les informations et processus doivent être accessibles aux personnes légitimes pendant les périodes prévues et avec le niveau requis de qualité.
- **Intégrité :** les informations doivent être protégées contre les modifications non autorisées qu'elles soient accidentelles ou volontaires.
- **Confidentialité :** les informations et fonctions doivent être accessibles uniquement aux personnes disposant des permissions nécessaires
- **Authenticité :** l'authenticité, la fiabilité et l'imputabilité des informations et fonctions doivent être assurées et pouvoir être testées.

7. Description du processus

7.1 Principes

- L'emploi des outils informatiques est lié à un but et n'est fondamentalement permis que dans l'accomplissement des tâches de service.
- Seuls pourront être utilisés, dans la société, des appareils dont celle-ci est propriétaire. L'emploi de matériels privés (par exemple un ordinateur portable privé) est fondamentalement proscrit. Il en va de même avec les logiciels rédigés en privé ou achetés en privé.
- L'utilisateur n'a pas le droit d'ouvrir l'appareil, de le manipuler ou de modifier la configuration du système. Seuls les collaborateurs du service informatique compétent sont autorisés à ouvrir le boîtier du PC et à effectuer des modifications sur celui-ci (par ex. installation et enlèvement des disques durs, lecteurs de disquettes, modules mémoires, etc.)
- De manière analogue, l'utilisateur s'interdit d'effectuer toute modification manuelle dans les fichiers système (il s'agit là, par exemple, des programmes et des données composant le système d'exploitation et les applications installées).

7.2 Description des règles d'utilisation des moyens informatiques

L'utilisation des moyens informatiques, informations, accès aux réseaux et services Internet est soumis au respect des règles énoncées dans le présent document, les procédures Volkswagen Bank France, la Politique de Sécurité des Systèmes d'Information et les lois en vigueur.

Le bon fonctionnement des systèmes d'information du Volkswagen Bank France suppose le respect des dispositions législatives et règlementaires qui s'imposent afin de garantir la sécurité,

la performance des traitements, la conservation des données professionnelles et la confidentialité des informations.

Les administrateurs systèmes et/ou réseaux de la direction des systèmes d'information (DSI) sont responsables techniquement de la sécurité et du bon fonctionnement des moyens informatiques et téléphoniques, placés sous leur responsabilité.

7.2.1 Principes de base

Le présent document est un code de bonne conduite fondé sur la Politique de Sécurité des Systèmes d'Information (PSSI). Il appelle à une attitude loyale, courtoise, responsable et respectueuse d'autrui dans l'intérêt de Volkswagen Bank, de ses clients et de ses utilisateurs.

7.2.2 Responsabilité

Chaque utilisateur est responsable de l'usage des moyens informatiques et des informations mis à sa disposition. Il s'engage à ne pas effectuer des opérations qui pourraient avoir des conséquences néfastes notamment sur le fonctionnement normal du réseau, sur l'intégrité des systèmes d'information, sur la sécurité des informations et sur l'image de marque de Volkswagen Bank. Cette responsabilité s'entend quel que soit le mode d'accès, sur site ou à distance.

Chaque directeur doit régulièrement informer les membres de l'équipe dont il a la charge, de leurs responsabilités en matière de sécurité des SI.

L'utilisation de ces moyens informatiques doit être rationnelle, conforme et loyale afin d'en éviter la saturation, le dysfonctionnement ou le détournement à des fins personnelles.

7.2.3 Utilisation professionnelle

Les moyens informatiques sont attribués à des fins professionnelles. Néanmoins, l'usage à des fins privées des moyens informatiques mis à la disposition du salarié, est toléré à condition que cet usage :

- soit occasionnel et raisonnable,
- n'entrave en rien la bonne conduite des affaires de Volkswagen Bank France,
- n'entrave pas la productivité,
- n'ait pas d'impact négatif sur l'image de Volkswagen Bank France,
- ne constitue pas une infraction aux présentes instructions,
- ne constitue pas une infraction aux lois françaises et internationales.

Les dispositions légales, le règlement intérieur, les contrats de travail s'appliquent pleinement même lors d'un usage personnel.

L'utilisateur qui souhaite utiliser, à des fins privées, les moyens informatiques mis à sa disposition est tenu de l'indiquer clairement grâce aux termes « Personnel » ou « Privé » dans le titre, l'objet ou l'intitulé. Cette mention doit obligatoirement apparaître dans le nom des fichiers ou répertoires ou dans le sujet des messages concernés.

Toutes les informations qui ne sont pas clairement identifiées comme « Personnel » ou « Privé », sont considérées comme des informations professionnelles.

7.2.4 Politique du bureau propre

L'utilisateur doit veiller à garder son bureau rangé. En particulier, il ne doit pas laisser sans surveillance des documents contenant des informations confidentielles.

Toute information confidentielle est soit stockée sous clé ou soit détruite dans les poubelles prévues à cet effet.

Les impressions correspondantes doivent être récupérées immédiatement.

7.2.5 Assistance

En cas d'incident ou d'anomalies, les utilisateurs doivent se rapprocher du département informatique selon la procédure Incident Management. Seul le département informatique est habilité à réaliser et à suivre les opérations de dépannage.

L'utilisateur concerné est chargé d'assurer l'accès des intervenants à son matériel, d'organiser le rendez-vous avec l'intervenant du département informatique et de l'informer des résultats de l'intervention.

Un incident lié à la sécurité de l'information survient lorsque des évènements non désirés ou imprévus menacent la vie privée ou la sécurité de l'information de l'entreprise. Ils peuvent être accidentels ou délibérés et incluent le vol, la perte, l'altération ou la destruction non autorisée de l'information.

Un incident lié à la sécurité de l'information est particulièrement critique lorsqu'il s'il s'agit d'une atteinte à la vie privée et que les données compromises contiennent des informations personnelles comme les noms, les dates de naissance, des données de santé ou financières, les numéros de sécurité sociale ou des renseignements de nature sensible.

L'honnêteté et la volonté de coopérer sont vitales dans le traitement des incidents de sécurité.
La clé d'une intervention appropriée en cas d'incidents liés à la sécurité de l'information est de prendre des mesures le plus tôt possible ! Les règles de conduite suivantes s'appliquent :

- **Rapporter et enregistrer l'incident**
  - Restez calme, ne faites aucune action dans la précipitation
  - Notez toutes les éléments constatés.
- **Informer**
  - Rapporter immédiatement les anomalies constatées aux référents dédiés.
  - Décrivez la situation exacte pour éviter d'autres dommages.
  - Donnez aux référents votre première estimation de la taille approximative des dommages, des conséquences, des parties concernées (Interne, Externe).

- **Mettre œuvre les mesures**
  - Suivre et appliquer les instructions fournies par les équipes sécurité et les administrateurs de la DSI.
  - Ne prendre en compte d'autres mesures que si elles proviennent de la cellule en charge de la résolution de l'incident.
  - Ne pas fournir d'informations à des tiers sans autorisation explicite.

Qui appeler

Problème / Incident	Contact
Incident majeur (qui affecte plusieurs utilisateurs)	Service Desk : 7333
Incident informatique qui affecte un utilisateur	Service Desk : 7333
Suspicion / **preuve** d'un incident de sécurité informatique (ex. virus)	Service Desk : 7333
Perte / Vol d'un support informatique physique ou d'informations appartenant à Volkswagen Bank France.	Service Desk : 7333
Questions relatives à la **protection des renseignements personnels**	VWFSFR, IT GRC <IT.GRC@fr.vwfsag.de>/ DPO (Data Protection Officer)
Questions générales concernant la **Sécurité informatique**	Intranet VWFSFR, IT GRC <IT.GRC@fr.vwfsag.de>

7.2.6 Participation aux actions de sensibilisation/formation à la sécurité des SI

L'entreprise met en œuvre des actions de sensibilisation ou de formation à la sécurité des systèmes d'information (par exemple : communication par email, quiz, questionnaire d'évaluation, jeux, simulation, formations en face à face, formation en ligne, etc.).

La participation à ces opérations est obligatoire.

La participation aux actions de sensibilisation s'effectue sur le temps de travail et est rémunérée comme du temps de travail effectif.

Dans le cadre de la sensibilisation, l'entreprise met en place une évaluation annuelle du niveau de sensibilisation à la sécurité des SI de ses salariés. Cela prend la forme d'un questionnaire d'évaluation que chaque salarié doit remplir.

Les résultats individuels de ces questionnaires sont utilisés pour déterminer les actions de sensibilisation appropriées pour l'entreprise et l'individu. Les résultats ne servent pas à l'évaluation de la performance individuelle et ne peuvent pas donner lieu à sanction ou bonification (le seul cas éventuel est le refus de participer à la sensibilisation).

La participation individuelle peut faire l'objet d'une communication à la hiérarchie dans un but de rappel de l'obligation de participation aux actions de sensibilisation.

Les personnes pouvant accéder aux résultats individuels du questionnaire d'évaluation sont :

- Le salarié lui même
- Le chef de service IT GRC et son équipe
- Le prestataire éventuel qui gère l'outil de sensibilisation
- La Direction des Ressources Humaines
- La hiérarchie

7.2.7 Consignes de sécurité

7.2.7.1 Sécurité des connexions et des accès

Connexion réseau

Seuls les postes de travail autorisés par la DSI de Volkswagen Bank France peuvent être connectés au réseau Volkswagen Bank France sans autorisation particulière.

Avec les ordinateurs n'appartenant pas à l'entreprise, une connection CITRIX doitêtre utilisée pour se connecter à distance au réseau d'entreprise. Un accès distance « VPN » peut être demandé pour les détenteurs d'un ordinateur portable de l'entreprise.

Contrôle d'accès logique

Le contrôle d'accès aux moyens informatiques de Volkswagen Bank France est lié à la possession d'un identifiant nominatif et unique ainsi que d'un mot de passe.

Le mot de passe doit respecter les règles de sécurité en vigueur (complexité, longueur, cycle de vie). Une fiche pratique est disponible sur l'Intranet pour aider l'utilisateur à choisir son mot de passe (cf. Annexe9.3).

Cet identifiant et mot de passe ne doivent en aucun cas être communiqués, prêtés, écrits ou divulgués pour quelque raison que ce soit.

En cas d'absence même temporaire de son poste de travail, l'utilisateur doit verrouiller sa session afin que d'autres utilisateurs ne puissent utiliser son poste et ses accès en son absence.

L'utilisateur ne doit pas usurper, emprunter ou encore tenter d'obtenir l'identifiant et mot de passe d'autres utilisateurs.

L'écran de veille doit s'activer automatiquement après un certain temps d'inactivité. Il doit demander un mot de passe pour se déverrouiller. Cela protège vos informations personnelles et les accès au réseau d'entreprise.

Dans la mesure du possible, vous devez éteindre votre ordinateur à la fin de la journée de travail.

7.2.7.2 Sécurité des informations

Documents de travail

Les documents électroniques de travail doivent être organisés, classés et répertoriés correctement afin de faciliter le partage s'il y a lieu, les sauvegardes et les impressions. Pour le partage de document, l'utilisateur doit utiliser les moyens informatiques mis à sa disposition.

Lors des impressions, l'utilisateur choisit une imprimante locale ou réseau qui garantit la sécurité de ses éditions. L'utilisateur doit les récupérer immédiatement.

Les documents inutilisés doivent être mis au rebus si possible à l'aide d'une broyeuse à documents ou dans des poubelles spécifiques aux documents confidentiels.

Sauvegarde des données

La sauvegarde des données stockées sur les postes de travail et les portables est de la responsabilité de l'utilisateur. Les données ainsi sauvegardées sur des périphériques externes doivent être stockées en lieu sûr et bénéficier d'un chiffrement adapté (cryptage).

La sauvegarde des données partagées stockées sur les serveurs, baies disques et espaces réseaux du groupe est de la responsabilité de la DSI. Les données professionnelles doivent être stockées sur ces espaces partagés mis à disposition.

7.2.7.3 Sécurité des moyens informatiques

Configuration matérielle et logicielle

La configuration du poste de travail ou des moyens informatiques ne peut être modifiée qu'en cas de nécessité professionnelle par la DSI ou avec accord de la DSI. Lorsque cette modification est effectuée par l'utilisateur lui-même, une dérogation doit être approuvée par le DSI.

Toute installation de matériel ou logiciel complémentaire doit être effectuée sous contrôle de la DSI en respectant les consignes de sécurité.

Toute installation et utilisation de logiciels, d'informations et d'œuvres au format numérique sera faite en respectant le cadre légal et les contrats de licences.

Postes nomades

Tout poste nomade (ordinateur portable, téléphone portable, smartphone) mis à la disposition d'un utilisateur est placé sous la responsabilité du détenteur et doit être utilisé dans le respect du présent document.

Le matériel de l'entreprise est réservé à un usage professionnel.

L'utilisation de filtre de confidentialité sur l'écran est obligatoire en dehors des locaux. Les tablettes et smartphone doivent être utilisé de façon à éviter qu'un tiers ne voie le contenu de l'écran.

Les matériels nomades sont fortement exposés au vol. Ils doivent être transportés dans les bagages à main durant les voyages. Ils doivent être protégés contre le vol (armoire à clé, câble antivol) quand ils doivent être laissés par exemple dans une voiture, un hôtel ou des salles de réunion.

Verrouillez l'appareil lorsque vous ne l'utilisez pas.

Les appareils mobiles ne doivent être synchronisés qu'avec des ordinateurs et logiciels approuvés par l'entreprise. La sauvegardes des données d'entreprise dans des systèmes externes tels que iCloud, dropbox, etc est interdite.

En cas de perte ou vol, suivez la procédure de déclaration d'incident de sécurité au plus vite. Remontez cet incident à votre manager.

Support amovibles

L'utilisation des supports amovibles est interdite. Cependant, un support chiffrée et agréé par le département des Opérations peut être mis à la disposition de l'utilisateur. Dans ce cas les règles suivantes doivent s'appliquer :

- L'utilisateur doit utiliser le support amovible dans le respect du présent document.
- En particulier la connexion de ce support est sous la responsabilité de l'utilisateur qui doit se protéger de tout risque notamment de virus informatique.
- Lorsque le support amovible est utilisé à des fins de sauvegarde, son stockage doit être sécurisé. L'utilisateur est responsable de celui-ci notamment en cas de vol, perte ou altération.

Obligation de surveillance du matériel confié

L'utilisateur a l'obligation de préservation du matériel qui lui est confié. En cas de dysfonctionnement de l'appareil mis à disposition, le service informatique a pour seule obligation de le remettre en son état initial, sans qu'il puisse lui être imputé des pertes de données.

Protection du matériel et des informations

La protection du matériel et des informations contre le vol, la copie et la dégradation doit être assurée en permanence. Les matériels portables doivent être attachés par un câble de sécurité ou rangés sous clé. Le câble de sécurité peut être obtenu auprès de la direction informatique. Le détenteur d'un matériel doit en permanence être en mesure de justifier de la propriété du matériel et des informations.

En cas de vol d'un matériel ou d'information et après le dépôt de plainte, le détenteur doit déposer une plainte auprès des autorités, informer immédiatement la direction des systèmes d'information et son responsable hiérarchique.

Restitution de matériel et de logiciel

La restitution des matériels informatiques doit avoir lieu dès la fin de la mission ou de l'activité concernée et doit comprendre l'ensemble des éléments prêtés. La DSI effectue une vérification de

conformité par rapport aux matériels et logiciels empruntés. La fiche de prêt est signée par la DSI et l'utilisateur pour validation et confirmation du retour.

Travail dans un lieu public

En cas de travail dans un lieu public (tel que une gare, un train, un avion ou dans la rue), l'utilisateur doit veiller à ne pas discuter d'informations confidentielles ou secrètes.

Il doit par ailleurs apposer un filtre de confidentialité sur son écran d'ordinateur afin de protéger celui-ci des regards indiscrets.

Le filtre de confidentialité peut être demandé auprès de la direction informatique.

7.2.7.4 Bon usage, cas particuliers

Utilisation de la messagerie

Dans le cadre de l'utilisation de la messagerie, l'utilisateur doit être sensible au fait que par défaut les informations transitent en clair sur Internet. En cas de besoin spécifique l'utilisateur doit contacter la DSI pour identifier la solution à mettre en place.

Tout message non identifié par la mention « Personnel » ou « Privé » dans l'objet est considéré comme professionnel.

Pour éviter de saturer les systèmes, l'utilisateur doit éviter les envois itératifs, répétitifs ou en grand nombre. Par ailleurs, l'utilisateur s'assure du respect de :

- La législation en vigueur, notamment du respect des tiers,
- L'image de marque de Volkswagen Bank France,
- L'identité des destinataires et de leur capacité à recevoir des messages,
- L'accord de son responsable hiérarchique, s'il y a lieu, pour cet envoi.

L'utilisateur doit être vigilant vis-à-vis des messages dont l'expéditeur est inconnu ou qui contiennent des pièces jointes ou des liens vers des sites Internet, et ne doit pas exécuter de programme, ouvrir de pièce jointe ou se connecter à des sites Internet dont il n'est pas sûr de l'origine. En particulier ne doit pas communiquer de façon inconsidérée son adresse de messagerie afin de ne pas être victime de spam.

L'utilisateur ne doit pas :

- Relayer des messages de fausse alerte,
- Participer à des chaînes de messages,
- Intercepter, modifier et transférer à d'autres personnes ni rendre publiques les communications qui ne lui sont pas adressées.

L'envoi de messages en masse ou à l'ensemble des collaborateurs est interdit sauf pour les personnes ayant reçu l'habilitation d'utilisation des listes de diffusion prévues à cet effet.

Logiciel de protection

La configuration des logiciels de protection contre les virus, les logiciels espions, les intrusions et autres attaques ne doit pas être modifiée.

Toute contamination devra être immédiatement signalée à la direction des systèmes d'information WVBK France selon la procédure d'assistance (cf. §7.2.5).

Utilisation d'Internet

Il est du devoir de l'utilisateur de respecter les consignes suivantes :

- Ne pas se connecter autrement que par les dispositifs mis en œuvre par la DSI sans autorisation explicite de ses responsables,

- Ne pas compromettre le bon fonctionnement des serveurs, des sites, des applications ou services auxquels il accède,
- Ne pas participer à des jeux ou des paris en ligne,
- Ne pas utiliser les services Internet à des fins malveillantes en rendant accessibles à des tiers des informations ou des données confidentielles ou contraires à la législation en vigueur,
- Ne pas déposer, copier ou transmettre des informations sur tout type de serveur sur Internet sans y être autorisé par les responsables habilités (propriétaires de l'information),
- Ne pas utiliser le cloud pour stocker des informations de l'entreprise,
- Ne pas autoriser les installations ou mises à jour de logiciels à partir de connexion Internet non sécurisées,
- En cas d'achat en ligne avec une carte bancaire, vérifier la sécurisation du site puis étudier attentivement ses relevés bancaires afin de signaler toute anomalie.

L'attention des utilisateurs est attirée sur le fait que la plupart des sites Internet qu'ils visitent gardent une trace de leur passage. Dans certains cas, ces sites identifient précisément la provenance du visiteur et son identité électronique (en l'occurrence, celle de Volkswagen Bank France lorsque les sites sont visités en utilisant l'accès Internet Volkswagen Bank France).

Utilisation des espaces de stockage

Des espaces de stockage sont mis à la disposition des utilisateurs sur les serveurs de Volkswagen Bank France. Ces espaces comportent des zones nominatives et des zones partagées. Ces espaces sont réservés au stockage de documents professionnels. La taille d'espace disponible pour chaque zone de stockage est limitée.

L'utilisation doit :

- Respecter les limites de taille définies et régulièrement archiver les documents inutiles ou obsolètes,
- Ne pas utiliser les espaces communs à des fins personnelles ou privées.

Utilisation du dossier temporaire ou dossier public

La DSI de Volkswagen Bank France met à disposition des utilisateurs un dossier temporaire (T:). Ce dossier ne doit pas servir à stocker de façon permanente des données ou exécuter des applications. En effet, les données de ce dossier sont effacées à intervalle régulier. Dans ce sens, l'utilisateur ne doit pas y stocker de données client ainsi que des données confidentielles. Cependant, les données publiques ou internes sont tolérées. De même l'utilisateur ne doit pas stocker ses données dans le dossier public propre au poste de travail.

7.2.7.5 Règles sur le transport de données

Le transfert de données se fait comme suit:

- Vous devez avoir l'accord du propriétaire de l'information avant de distribuer une information confidentielle ou secrète
- Vous devez chiffrer l'envoie d'informations confidentielles ou secrètes vers des tiers
- Ne laissez pas d'information confidentielle ou secrète sur une boite vocale
- N'utilisez pas le fax
- Allez chercher immédiatement à l'imprimante vos impressions de documents confidentiels ou secrets

La contribution à des forums, groupes de discussions sur Internet sont soumises aux même règles que la publication d'article ou d'opinions au nom de Volkswagen Bank France. Elle doivent être approuvée par la personne en charge des relations presse.

7.2.7.6 Chiffrement des données confidentielles

Les données confidentielles doivent obligatoirement disposer d'un chiffrement (cryptage) adapté lors de leur stockage et de leur tranfert. Ceci est particulièrement vrai lors de l'échange d'informations confidentielles par le biais de la messagerie électronique ou encore lors de leur transfert via des supports amovibles (seule l'utilisation de la clé USB sécurisée Volkswagen Bank France est autorisée).

La capacité de chiffrement des outils de compression tels que 7zip peut être utilisée pour protéger les informations non publiques pour les transmettre aux autres compagnies ou si le système de messagerie de Volkswagen Bank France n'est pas utilisé. Dans ce cas, le mot de passe utilisé doit être communiqué par un autre canal de communication (ex. téléphone). Un mot de passe ne doit pas être utilisé plus d'une fois.

7.2.7.7 Règles sur la classification des informations

Chaque utilisateur se doit, lors de la création d'un document, d'y apposer un niveau de classification. Les règles permettant de déterminer le niveau de classification et les actions qui en découlent sont précisées dans la Politique de classification de l'information.

7.2.7.8 Gestion des absences ou des départs définitifs

En cas d'absence ou de départ définitif de l'entreprise, l'utilisateur est tenu de communiquer à sa hiérarchie les données et informations nécessaires à la poursuite de l'activité de la société.

En cas d'impossibilité ou de refus de la part de l'utilisateur, l'entreprise peut prendre les mesures nécessaires pour accéder aux données professionnelles contenues sur les ressources informatiques et/ou services internet de l'intéressé.

Il appartient à l'utilisateur lors de son départ définitif de l'entreprise de sauvegarder ses données privées puis de les détruire. Au cas où les circonstances du départ ne permettraient pas d'atteindre cet objectif, l'entreprise conservera une sauvegarde de ses fichiers pour une durée de 30 jours calendaires sans engagement de résultat.

7.2.7.9 Données personnelles

Les données personnelles se réfèrent à des données spécifiques concernant les affaires personnelles ou objectives d'une personne physique identifiée ou identifiable. Ceci inclut les informations sur les employés, les clients ou des tiers de l'entreprise qui sont stockées et conservées par VW Bank France. Les données personnelles comprennent entre autres :

- Nom, adresse, date d naissance, numéro de téléphone, adresse électronique
- Age, sexe, état civil
- Numéro de compte, solde bancaire, salaire
- Les catégories particulières de données à caractère personnel incluent couleur, origine nationale ou ethnique, religion
- Les croyances politiques, philosophiques ou religieuses
- La santé ou l'orientation sexuelle

7.2.7.10 Espace personnel

Un usage personnel raisonnable des outils informatiques est toléré par l'Entreprise. Pour cela, l'utilisateur doit stocker ses données (fichiers et messages électroniques) dans le dossier réseau P, dans un dossier appelé « Personnel » dans le dossier Mes Documents du poste de travail ou

dans sa messagerie et ses archives de messagerie. L'entreprise s'interdit d'accéder à ces données en dehors de la procédure définie (Cf. § 7.3.4)

Toute donnée stockée en dehors de ces espaces sera présumée professionnelle et pourra être accédée librement par l'Entreprise.

7.2.7.11 Restriction

La direction des systèmes d'information se réserve le droit de ne plus assurer ses services ou d'en restreindre l'usage en cas de non-respect du présent document.

7.2.8 Interdiction

D'une manière générale, sont strictement interdits :

- la diffusion d'informations confidentielles relatives à Volkswagen Bank, à ses clients, à ses partenaires ou aux salariés, sauf si la conduite des affaires le requiert raisonnablement et avec l'accord de la hiérarchie ;
- la diffusion de messages, enquêtes ou publicités politiques, racistes, ou de propagande ;
- la diffusion, le stockage ou le téléchargement d'informations ou d'œuvres en infraction avec le droit d'auteur ;
- l'accès ou le stockage de publications à caractère injurieux, diffamatoire, raciste, pornographique, de harcèlement sexuel/moral, ou tout autre contravention ou délit d'ordre pénal ou civil ;
- l'atteinte à tout signe distinctif appartenant à des tiers, en particulier aux droits de marques, notoires ou non, à toute dénomination sociale, enseigne, nom commercial et nom de domaine ;
- l'accès aux données personnelles d'une tierce personne sans l'autorisation de celle-ci ;
- l'accès aux données communes ou partagées de Volkswagen Bank sans l'autorisation des personnes habilitées ;
- l'altération, la copie ou la suppression des informations appartenant à une tierce personne, à Volkswagen Bank France ou à un client ;
- la mise à disposition d'utilisateurs non autorisés un accès aux systèmes ou au réseau quel que soit le type de matériel employé.

Tout contrevenant à ces interdictions considérées comme substantielles engage sa responsabilité et en assume les entières conséquences légales et financières.

D'une manière générale, l'utilisateur doit prendre conscience que ces traitements non professionnels sollicitent inutilement les ressources des moyens informatiques, le plus souvent partagées.

7.2.9 Prestataires, outsourcing et acquisitions de logiciels

Le PC guideline s'applique aux prestataires disposant d'un accès au SI.

Toute personne faisant appel à des prestations ou des services externes est responsable de s'assurer de la conformité du prestataire avec la Politique de Sécurité des Systèmes d'Information (PSSI) ainsi qu'à la Politique des Achats et la Politique d'Outsourcing de Volkswagen Bank France notamment l'IT Minimum Standard. Cela doit se traduire par l'existence de clauses contractuelles adaptées.

Le choix et l'acquisition de logiciel est de la responsabilité de la DSI. Les achats hors DSI ne sont pas autorisés. Au cas où cela se produirait, le métier ayant réalisé l'acquisition est responsable de

la conformité du logiciel avec la politique de sécurité et assumera la mise en conformité éventuelle du logiciel.

7.2.10 Cas dérogatoires

Dans le cadre de son activité professionnelle, l'utilisateur peut demander des dérogations concernant le présent document.

La demande doit être émise par le supérieur hiérarchique ayant autorité et comporter les éléments suivants :

- La tache ou la fonction justifiant la dérogation,
- La durée souhaitée pour cette dérogation.

Après obtention de ces informations, un accord officiel du Responsable de la Sécurité des SI sera nécessaire afin de valider la dérogation.

7.3 Exploitation des moyens informatiques

Ce paragraphe concerne les droits et devoirs des personnels informatiques disposant d'accès privilégiés au système d'information (ci-après administrateurs techniques)

7.3.1 Obligation de discrétion

Afin de garantir le bon fonctionnement et la sécurité des moyens informatiques de Volkswagen Bank France, un nombre réduit de personnes, chargées de leur administration dispose d'un accès privilégié sur ceux-ci. Ces personnes encore nommées administrateurs techniques ont notamment la possibilité d'accéder aux fichiers et courriers électroniques stockés et échangés.

Conformément aux lois en vigueur dont la loi 78-17 relative à l'informatique, aux fichiers et aux libertés, ces personnes sont soumises à une obligation de secret professionnel. Elles ne peuvent en aucun cas exploiter à des fins autres que celles liées au bon fonctionnement et à la sécurité des moyens informatiques, les informations dont elles auraient eu connaissance.

7.3.2 Obligation de discrétion, cas de force majeur

En cas de force majeure, le management (Directeur) peut demander à la Production informatique l'accès aux informations ou aux boites aux lettres d'utilisateurs. Dès lors, l'administrateur technique prend la responsabilité de respecter les lois en vigueur (notamment le code du travail et la loi informatique et libertés). L'administrateur technique doit respecter le caractère personnel des informations dès l'instant qu'il est explicitement indiqué.

7.3.3 Droits et devoirs spécifiques des administrateurs techniques

Les administrateurs :

- ont la charge de la bonne qualité des services de la DSI fournis aux utilisateurs de Volkswagen Bank France dans la limite des moyens alloués. Ils ont le droit d'entreprendre toute démarche nécessaire au bon fonctionnement des moyens informatiques de Volkswagen Bank France en accord avec le LISO.
- ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.
- ont le devoir d'informer immédiatement le LISO de Volkswagen Bank France de toute tentative d'intrusion sur un système, ou de tout comportement délictueux d'un utilisateur.

- ont l'obligation de préserver et de respecter la confidentialité des informations privées qu'ils sont amenés à connaître dans le cadre de leur activité.
- doivent avoir la connaissance et la maîtrise de tous les équipements informatiques et réseaux appartenant au sous-réseau qu'ils gèrent. Ils doivent tenir à jour la liste des équipements (machines, routeurs, imprimantes, . . .) et des prises réseaux (localisation, utilisateur connecté à la prise).
- doivent inspecter régulièrement les fichiers de traces de manière à détecter le plus vite possible toute intrusion. Toute création de nouveau service, ouverture de nouveaux ports doit être validée selon les processus de validation de la DSI
- ont le devoir d'appliquer les correctifs nécessaires aux applications qui présentent des failles de sécurité.
- ont le devoir de s'informer régulièrement sur les menaces qui pèsent sur le SI de Volkswagen Bank France et des mesures de sécurité mises en place par l'entreprise.
- Doivent respecter les dispositions définies dans l'IT Minimum Standard.

7.3.4 Prise en main à distance

Les logiciels de prise de main à distance permettent notamment aux administrateurs d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique.

Ces outils de télémaintenance ou de prise de main à distance ne doivent en aucun cas être utilisés à des fins de contrôle de l'activité des utilisateurs. Une telle utilisation n'étant ni conforme au principe de proportionnalité, ni respectueuse du principe de finalité posé par la loi « informatique et libertés ».

Dans l'hypothèse d'un recours à ces outils à des fins de maintenance informatique par un administrateur, leur utilisation doit s'entourer de précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquelles le gestionnaire technique accédera par ce moyen, dans la stricte limite de ses besoins.

Doivent notamment figurer au titre de ces précautions :

- l'information préalable et le recueil de l'accord de l'utilisateur pour « donner la main » à l'administrateur informatique avant l'intervention sur son poste (à titre d'illustration, l'accord peut être donné par simple validation d'un message d'information apparaissant sur son écran) ;
- la traçabilité des opérations de maintenance (par exemple, par la tenue d'un registre des interventions), ainsi que la précision dans les contrats des personnes assurant la maintenance - notamment en cas de recours à des prestataires extérieurs - de leur obligation de n'accéder qu'aux données informatiques nécessaires à l'accomplissement de leurs missions et d'en assurer la confidentialité.

7.4 Obligations

7.4.1 Obligations générales

L'utilisateur :

- doit assurer la protection des informations auxquelles il a accès (confidentialité et intégrité) et est responsable des droits d'accès qu'il donne aux autres utilisateurs,
- doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater.

7.4.2 Obligations légales

7.4.2.1 Déclaration à la CNIL

Si l'utilisateur est amené à constituer des fichiers soumis aux dispositions de la loi informatique et libertés, dans le cadre de son activité professionnelle, il doit accomplir les formalités requises par la CNIL par l'intermédiaire du correspondant CNIL de Volkswagen Bank France en concertation avec son management et veiller à un traitement des données conforme aux dispositions légales.

7.4.2.2 Propriété intellectuelle

L'utilisateur doit respecter les dispositions de la loi sur les Droits d'Auteur et les Droits Voisins de la Société Informatique qui encadre les œuvres sous un format numérique, les logiciels et les informations. Tout téléchargement illégal est prohibé.

7.4.2.3 Informations personnelles

L'utilisateur dispose d'un droit d'accès, de modification et de suppression des informations à caractère personnel le concernant conformément aux dispositions légales.

Il doit s'adresser à la DRH.

7.4.2.4 Information

Le présent document conformément à l'article L122-36 du code du travail a été soumis pour avis aux institutions représentatives du personnel. Les modifications ultérieures seront également soumises pour avis.

7.4.3 Confidentialité et accès aux fichiers

La consultation, la modification ou la destruction d'informations détenues par d'autres utilisateurs sont interdites. Elles ne peuvent être réalisées qu'après accord explicite de l'utilisateur responsable de la gestion de ces informations quand bien même les utilisateurs ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées par messages électroniques dont l'utilisateur n'est destinataire, ni directement, ni en copie.

En cas d'urgence et notamment pour assurer la sécurité et l'intégrité du système d'information ou la continuité du service, le management peut être amené à passer outre ces règles si l'utilisateur concerné n'est pas en mesure de donner son accord dans les délais requis. Cette exception ne peut concerner que les fichiers susceptibles d'être la cause des anomalies constatées ou requis pour la continuité d'activité. Ces interventions sont exceptionnelles et font l'objet d'une information de l'utilisateur.

Dans le cas où les fichiers recherchés seraient situés dans un espace personnel, la consultation se fera soit :

- En présence de l'utilisateur
- En présence d'un membre des instances représentatives du personnel ou d'un officier de police judiciaire en cas d'absence ou refus de l'utilisateur ou cas de risque avéré pour l'entreprise.

7.5 Audit et contrôles

Pour assurer le bon fonctionnement des moyens informatiques de Volkswagen Bank France, il est procédé à des audits et à des contrôles automatisés, dans le respect de la confidentialité et de la vie privée des utilisateurs. En particulier, Volkswagen Bank France met en œuvre sur les systèmes les contrôles récurrents suivants :

- Réseau : filtrage et écoute (à fin de résolution d'incidents ou optimisation) du trafic réseau,
- Réseau : traces de connexion,
- Internet : audit des sites visités et du trafic par utilisateur,
- Internet : filtrage de l'accès aux sites illégaux, présentant des risques de sécurité ou à caractère non professionnel,
- Messagerie électronique : contrôle antispam et filtrage de la messagerie,
- Messagerie électronique : traçabilité des objets et destinataires des messages par émetteur,
- Internet et messagerie : trace des sites consultés et des messages échangés (sans le contenu),
- Fichiers : surveillance des taux d'utilisation des espaces de stockages personnels et communs,
- Fichiers : trace des accès aux fichiers
- Global : contrôle des virus, codes malveillants et fuites d'information

Lors de ces audits, l'ensemble des informations présentes peuvent être analysés par les outils automatiques y compris les fichiers personnels. La procédure précédemment décrite reste applicable en cas de besoin d'accéder à ces fichiers par un administrateur.

Les instances représentatives du personnel seront consultées et les utilisateurs informés si d'autres audits devaient être mis en œuvre.

7.6 Respect des règles et sanctions encourues

Chaque utilisateur doit se conformer à la politique de sécurité des SI (PSSI) de l'entreprise.

Les règles exposées dans le présent document impliquent une attention particulière, leur non-respect étant susceptible d'entraîner des sanctions prévues dans le règlement intérieur ou des poursuites civiles et/ou pénales conformément à la législation en vigueur en fonction de la gravité des faits reprochés et/ou de leurs conséquences sur le préjudice subi par Volkswagen Bank France.

Volkswagen Bank France se réserve le droit de prendre toute mesure pratique dans le respect du cadre légal afin d'établir les responsabilités en cause et d'empêcher toute utilisation irrégulière ou illégale des systèmes.

Il est rappelé que les droits d'accès aux moyens informatiques ainsi que les conditions d'utilisation sont accordés à chaque utilisateur en considération stricte des fonctions qu'il occupe. L'utilisateur est informé que toute tentative de s'arroger des accès indus à des systèmes informatiques, toute manipulation technique déloyale ou divulgation d'informations préjudiciables à un tiers ou à Volkswagen Bank France, tout usage volontairement contraire aux règles internes ou aux lois constituent une faute pouvant entraîner des sanctions et engager sa responsabilité individuelle.

8. Contrôle Interne

Opérateur	Ressources Humaine (pour les internes) Chef de départements (pour les externes)
Objectifs du contrôle	Tous les collaborateurs (internes ou externes) qui ont accès à des informations non publiques de l'entreprise sont informés des exigences de sécurité pour le traitement des informations de la Société avant de recevoir un compte informatique.
Contrôle	Chaque employé qui signe un contrat de collaboration avec Volkswagen Bank France doit disposer de cette procédure en complément de son contrat. Il doit confirmer par écrit la lecture de cette procédure. Cette confirmation écrite doit être stockée dans son dossier par les Ressources Humaines. Les prestataires externes de Volkswagen Bank France doivent recevoir cette procédure de la part du département contractant leur prestation. Ils doivent confirmer sa lecture par écrit. Cette confirmation écrite doit être stockée dans le dossier du projet par le département contractant. Le prestataire doit conserver une copie de la confirmation écrite. Les prestataires externes travaillant pour plusieurs départements doivent signer une confirmation pour chaque département. Cependant, ils peuvent présenter la confirmation déjà signée dans un autre département.
preuve	Confirmation écrite
Délai	Avant que les informations du compte informatique ne soient transmises au nouveau collaborateur.
Lieu de stockage	Dossier personnel (employé interne), Dossier du projet (prestataire externe)
Durée du stockage	2 ans après la fin de la collaboration

9. Annexes

9.1 Contacts

Service IT GRC • IT Compliance • Information Security • IT Risks • AIM • Enterprise Architecture	VWFSFR, IT GRC <IT.GRC@fr.vwfsag.de>
Data Protection Officer	VWFSFR, RGPD <vwfs.dpo@fr.vwfsag.de>

9.2 Trucs et astuces

Vous trouverez sur l'intranet des fiches pratiques sur des sujets tels que le choix du mot de passe ou le verrouillage de la station.

9.3 Caractéristiques du mot de passe

Votre mot de passe de doit être connu que de vous, il doit être assez complexe pour ne pas être facilement deviné. Les règles suivantes s'appliquent (se référer également au Manuel des Organisations des Banques Européennes (OMEB) Régulation Passwords Requirements)

TYPE	REGLE

Cas général	• Les mots de passe doivent contenir :
	  ○ Au moins 10 caractères
	  ○ Au moins une majuscule
	  ○ Au moins une minuscule
	  ○ Au moins un chiffre
	  ○ Au moins un caractère spécial (:$/<>* ?;- !=, etc.)
	• Les mots de passe ne doivent pas contenir un mot ou une information liée à l'utilisateur (nom, date de naissance, etc.)
	• Changer immédiatement votre mot de passe initial
	• Les mots de passe doivent être changés régulièrement (tous les 90 jours)
	• Le nouveau mot de passe ne doit pas être identique aux six précédents
	• Le mot de passe ne peut être changé qu'une fois toutes les 48 heures
	• Le compte est bloqué après 5 erreurs d'authentification (le compteur peut être réinitialisé quotidiennement)
	• Ne Divulguez (communiquez, notez, sauvegardez en texte clair, etc.) pas votre mot de passe à des tiers.
	• Gader votre mot de passe secret

Clients et partenaires	• Les mots de passe contiennent au moins 10 caractères • Les mots de passe peuvent avoir une durée de vie de 180 jours maximum • Le nombre d'essais du mot de passe peut être porté à 30 après validation du service IT GRC et du Métier
Administrateurs, comptes de service	• Les mots de passe contiennent au moins 16 caractères • Les mots de passe doivent être changés régulièrement

9.4 Types de menaces (en anglais)

Identity theft/identity fraud - Identity theft is fraud. This occurs when another person uses your personal information without your knowledge or consent to commit a crime. Fraud may involve using your credit card for a few transactions, selling your information in the underground economy, or establishing a separate identity that may include obtaining a loan, buying a home, buying goods and services, or traveling over a period of time, on your behalf and without your knowledge. Your personal data, including your VW Bank France ID (DKX) and password, can be stolen from the Internet in different ways.

Malicious code or malware - Malicious code is the term used to describe software (a computer program) designed to exploit, infiltrate or damage a computer system without the informed consent of the user. It is also called "malware" and includes computer viruses, worms, Trojans, rootkits, spyware, dishonest advertising software and other unwanted software. Malicious codes are usually distributed over the Internet, by email or via compromised web pages.
See chap **Error! Reference source not found.** for a list of some currently widespread malicious software**.**

Internet hoaxes - Internet hoaxes are the email equivalent of letter chains. They are disclosed to others through a hyperlink, email or even a chain letter. They are also effective in their highly manipulative content, which exploits emotions to create a bond of trust with victims. The purpose of sending these emails is to install malicious code and/or to enter personal and financial information or the names and email addresses of the recipient's contacts when the email is forwarded. Hoax emails contain messages that are generally false and usually contain warnings about computer viruses or allegedly dangerous products or they present tragic stories or calls for financial help. You may receive an email informing you that you have won a lottery or contest to which you did not participate…

Spam - Spam accounts for the vast majority of emails sent worldwide every day. Internet hoax emails are spam, as are mass marketing emails that try to sell products at very attractive prices that are counterfeit (e.g. over-the-counter prescription drugs, branded products such as handbags, shoes and jewelry, and even antivirus software and university degrees). Spam is almost always offers that are "too good to be true", which should serve as a warning in itself. It is usually because of these allegations, however, that people are welcomed and robbed through unsolicited emails. Never click on the links in these emails. Unsolicited emails should be deleted without opening and never sent to others. (You can use the automatic preview functions or ...)

Phishing - Email phishing is a common type of online fraud, identified as one of the main Internet threats used for credit card fraud and identity theft. Phishing attempts to trick people into disclosing credit card numbers or online banking information. The method is to send a fake email that appears to be from a legitimate and trustworthy source, such as a bank or other financial institution, an online shopping company or a support center. The email asks the recipient to enter their financial information (credit or debit number and password) or proof of identity (username or account number and password) because of a problem, thus addressing the person's concerns about their personal information. VW Bank France's firewalls are constantly updated to block phishing attempts and spam.

Social Engineering - Social engineering is the practice of obtaining information or access by trapping legitimate innocent users. Social engineers use the "shoulder-surfing" technique, i.e. looking over a person's shoulder to steal information, phone calls or emails to obtain sensitive details, exploiting the a person's natural tendency to trust others.
In general, it is easier to take advantage of a person in this way, rather than trying to exploit computer security vulnerabilities. Many major breaches against businesses around the world began with an employee inadvertently providing information that allowed cyber criminals to access it. Beware of unsolicited phone calls or emails requesting personal information or information....

9.5 Types de logiciels malveillants (en anglais)

Viruses and Worms - A computer virus is a computer program that can be copied and infected with a computer. A virus that replicates itself by referring to an attachment to an email or network message is known as a worm. Both can delete or modify files or overload networks.

Trojans –It is a Trojan horse, a program in which malicious or harmful code is contained in a seemingly harmless programming or data in such a way that it can take control and cause damage by installing a "backdoor", allowing outsiders to access and control your computer. **Keystroke Recorder** - A keystroke recorder, sometimes called a keystroke recorder or system monitor, is a hardware device or small program that monitors every keystroke that a user taps on a specific computer keyboard, records everything that is typed (including passwords) and transmits this information to third parties (usually via Bluetooth or similar technology). Key recorders can be purchased in retail stores and legally installed on home computers, for example, to monitor children's use

Spyware -Spyware is a technology that helps collect information about an individual or organization without their knowledge. On the Internet, spyware is any piece of software or set of instructions that are placed on a person's computer to secretly collect their data (such as browsing history) and pass it on to advertisers or other interested parties. Spyware can enter a computer in the form of a software virus or as a result of installing a new program on the computer.

Rootkits -A rootkit is a set of tools (programs) that allows the administrator to access a computer or computer network and control, attack or collect your information. They often operate silently on computer systems and are usually not detected by anti-virus or anti-spyware software.

Botnet - A botnet is a network of computers that communicate with other similar programs for performing certain tasks including the transmission of spam or viruses without the knowledge of owners.