Charte utilisateur téléphones mobiles et clés 3G/4G

1 Objet de la charte

Tout personnel de l'Université de Bretagne Occidentale (UBO) attributaire d'un moyen de communication mobile (téléphone ou clé 3G/4G) de la propriété de l'UBO doit prendre connaissance de cette charte et s'engager à respecter les règles de bon usage qu'elle contient.

A l'attribution de l'appareil, il reconnait en avoir pris connaissance et en accepter les conditions.

2 Diffusion du numéro de mobile

Tout agent disposant d'une attribution de téléphone mobile doit communiquer son numéro à qui de droit :

- au minimum, à son supérieur hiérarchique direct, au directeur de la composante ou du service, au responsable administratif,
- dans les procédures spécifiques de sécurité,

L'agent doit être joignable sur ce numéro de mobile durant ses heures de travail et d'astreinte.

3 Utilisation professionnelle - matériel

Le titulaire d'un téléphone mobile de l'UBO ou d'une clé 3G/4G utilise ceux-ci dans un cadre professionnel et qui s'inscrit conformément à ses fonctions pour lequel il reçoit le dit mobile ou clé 3G/4G. S'il quitte ses fonctions, l'agent doit impérativement rendre son téléphone mobile et/ou sa clé 3G/4G au gestionnaire du parc mobile et en aucun cas l'attribuer à un autre agent, même si celui-ci est son successeur.

Seul le service gestionnaire du parc mobile est habilité à réattribuer un téléphone mobile ou/et sa clé 3G/4G.

Pour des questions techniques, d'accompagnement et d'homogénéisation du parc, le choix de l'appareil sera du ressort du gestionnaire du parc mobile en fonction des besoins définis par le demandeur.

L'attributaire s'engage à prendre soin du matériel qui lui est confié nominativement et qui est placé sous sa responsabilité personnelle.

Il est réputé avoir la garde du téléphone mobile remis. Il s'engage à signaler au gestionnaire du parc mobile via l'adresse mobile@univ-brest.fr, tout incident, perte, vol ou casse et également à son responsable hiérarchique pour solliciter un nouvel appareil.

La fourniture d'accessoires supplémentaires « kit mains-libres », « prise allume-cigare », sacoche ou tout autre élément annexe au mobile ne sont pas pris en charge ni délivrés.

Les appareils mobiles ou les clés 3G/4G restent la propriété de l'UBO : ils peuvent donc être repris ou remplacés par d'autres modèles à l'initiative de l'UBO.

En cas d'utilisation d'un téléphone mobile personnel avec un forfait téléphonique professionnel fourni par l'université, le titulaire s'engage à respecter les termes de cette charte relevant du bon usage du forfait. Il est déchargé des engagements concernant son mobile personnel.

4 Utilisation professionnelle - consommation

Le titulaire d'un téléphone mobile de l'UBO ou d'une clé 3G/4G s'engage à avoir une utilisation raisonnée des communications et en particulier à rester vigilant lors de l'utilisation des options DATA (transfert de données, messagerie, internet...), notamment lors des déplacements à l'étranger (la possibilité de désactiver l'option "données à l'étranger" existe).

L'annexe 4 décrit les tarifs des communications (voix, SMS/MMS et data) pour la France métropolitaine et l'international valables sur la durée du marché soit jusqu'au 16 juin 2019.

Toute modification du forfait (ajout ou suppression d'option) devra être au préalable autorisée par le responsable hiérarchique après sollicitation du responsable des crédits. Ces demandes sont à adresser au gestionnaire du parc mobile lequel sollicitera le cabinet pour les demandes concernant les directeurs des composantes et des laboratoires et le DGS pour les autres cas.

5 Utilisation du WIFI versus la clé 3G/4G

Pour des questions de coût, l'utilisateur doit privilégier la connexion WIFI plutôt que la connexion en clé 3G/4G de l'opérateur notamment sur les sites de l'enseignement supérieur en Europe. Il est recommandé de se connecter au réseau EDUROAM avec l'identifiant UBO ("identifiant ENT"@univ-brest.fr) et le mot de passe ENT. La documentation complète est disponible sur le site de la DSI, onglet « Documentations », rubrique « Accès réseau, internet et wi-fi »

6 Suivi de la consommation / comptabilisation

Les coûts des communications seront refacturées pour les composantes et les laboratoires à chaque fin d'année civile.

Les dépassements de forfait liés sont très vite onéreux d'où la vigilance demandée. A l'attribution du mobile, l'agent est sensibilisé à l'usage professionnel requis à la lecture de la présente charte. Le gestionnaire du parc mobile sous la responsabilité du Directeur Général des Services se réserve le droit de signaler les dépassements éventuels et de conseiller d'éventuels changements de forfait ou de paramétrage.

Le WIFI doit être privilégié pour les usages DATA (transfert de données, messagerie, internet...) [cf. point 5].

En cas d'utilisation non professionnelle occasionnant un dépassement important du forfait alloué ou des consommations hors forfait, l'université se réserve le droit d'étudier toutes les mesures adéquates correctives et éventuellement d'engager une demande de remboursement de la contre-valeur.

7 Sécurité

L'activation de l'application qui sur votre demande, protègera à distance votre Smartphone en cas de vol, est vivement recommandée. Elle permettra l'effacement à distance de vos données personnelles. Cela restaurera les réglages d'usine de votre mobile. Pour la mise en place de cette fonctionnalité sur votre smartphone, reportez-vous à l'annexe 1.

Une attention est portée aux comportements dangereux comme le téléchargement d'applications "exotiques", venant de sources non sûres ou l'utilisation de modes de paiements non sécurisés.

La perte ou le vol d'un équipement (ou d'un support) mobile ou nomade peut être lourd de conséquences pour l'université : en l'absence de chiffrement, les données stockées sur le terminal (patrimoine technologique) seront en effet compromises. Le risque de fuite d'informations est encore plus grand de par les nombreuses fonctionnalités présentes sur les ordiphones et les tablettes. Il convient de le prendre en compte sérieusement dans un contexte professionnel. Un attaquant pourra par exemple chercher à pénétrer le système d'information de l'UBO en utilisant comme point d'entrée un terminal mobile. Cela est dû principalement à la multitude de vulnérabilités que présentent les systèmes d'exploitation mobiles. Pour la mise en place de la fonctionnalité "chiffrement de données" sur votre smartphone, reportez-vous à l'annexe 2.

Recommandations de sécurité relatives aux ordiphones de l'Agence Nationale de la Sécurité des Systèmes d'Information (note DAT-NT-010/ANSSI/SDE/NP du 28 juillet 2015).

R2 : Configurer une durée d'expiration du mot de passe de 3 mois maximum.

R3 : Configurer le verrouillage automatique de terminal au bout de 5 minutes maximum.

R4 : Si le terminal contient des informations sensibles, il est recommandé d'exiger un mot de passe fort en remplacement des méthodes de déverrouillage par défaut. Dans tout autre cas, l'utilisation d'un code PIN sera suffisante dès lors que la recommandation R5 est strictement respectée.

R5 : Limiter le nombre de tentatives de déverrouillage, puis configurer un temps de blocage de plus en plus long ainsi qu'un effacement automatique après une dizaine de tentatives ayant échoué.

R6 : Ne pas laisser le terminal sans surveillance. Un accès très temporaire à un terminal mobile peut suffire à sa compromission sans que l'utilisateur en ait conscience même lorsqu'il est verrouillé.

R7 Ne pas brancher le terminal à un poste de travail non maîtrisé ou à un quelconque périphérique qui ne soit pas de confiance, lesquels établiront une connexion directe non contrôlée.

R11 : L'accès au service de géolocalisation doit être interdit aux applications dont les fonctions liées à la position géographique ne sont pas utilisées. Si cette option n'est pas disponible sur le terminal considéré, il convient d'éteindre le service de géolocalisation lorsqu'il n'est pas utilisé.

R13 : Les applications déployées doivent être mises à jour régulièrement et rapidement dès lors que des correctifs de sécurité sont proposés.

R14 : Les interfaces sans-fil (Bluetooth et WiFi) ou sans contact (NFC par exemple) doivent être désactivées lorsqu'elles ne sont pas utilisées.

R15 : Désactiver systématiquement l'association automatique aux points d'accès WiFi configurés dans le terminal afin de garder le contrôle sur l'activation de la connexion sans-fil.

R16 : Éviter tant que possible de se connecter à des réseaux sans fil inconnus et qui ne sont pas de confiance.

Il est interdit de « jailbreaker » ou « rooter » les smartphones. Pour de plus amples informations, reportez-vous à l'annexe 3.

Le Président de l'Université
de Bretagne Occidentale

UNIVERSITÉ DE BRETAGNE OCCIDENTALE

Annexe 1 : Effacement de vos données personnelles à distance

Pour les Apple, activer « Localiser mon iPhone » dans la rubrique « Réglages\Icloud » et pour les Android, activer «Gestionnaire d'appareils Android » dans « Paramètres Google ».

Annexe 2 : Chiffrement des données

Il est important de chiffrer les données sensibles. L'activation de cette fonctionnalité est automatique sur les iPhone depuis la version 8.0 et depuis Android Marshmallow (la version 6 d'Android). Sinon, il faut se rendre dans la section Réglages de votre téléphone Android puis sélectionnez Sécurité (ou Paramètres puis Paramètres avancés).
Il faut au préalable activer le verrouillage de votre écran par un mot de passe (code PIN) ou un motif qui sécurisera votre appareil. Cela implique que personne ne pourra accéder à votre téléphone sans votre code personnel.
Pour activer le verrouillage de l'écran, il vous suffit de vous rendre dans les Réglages (ou Paramètres selon les versions d'Android) de votre téléphone (le plus souvent représentés par l'icône d'une roue dentée) puis l'onglet Sécurité, et de choisir la façon de verrouiller votre écran (avec un code PIN, un mot de passe ou un motif). Pour les iPhone, il vous suffit de vous rendre dans le menu Réglages puis l'onglet « Touch ID et code ».
Il convient de se rapprocher de votre gestionnaire de parc mobile pour mettre en œuvre la technologie de chiffrement la plus adaptée en fonction du terminal et des données à protéger.

Annexe 3 : « jailbreaker » ou « rooter »

Cette méthode consiste à débrider le mobile pour en avoir le contrôle total et l'utiliser au-delà des limites imposées par le constructeur. Il ne faut pas confondre avec le « désimlock, qui autorise l'utilisation de son appareil via n'importe quel opérateur ». Comme son nom l'indique, le désimlock agit sur la carte SIM. Le jailbreaking ou rooté agit directement sur l'appareil.