ALGERIAN UNION BANK بنك الاتحاد الجزائري — ثقة LA CONFIANCE SANS FRONTIÈRES	REFERENCE DE LA PROCEDURE	DATE DE CREATION	Version
	Charte N° 02 /2023	14/11/2023	01

Charte de Sécurité des Systèmes d'Information

Diffusion Générale

Signature

Algerian Union Bank — Direction Générale — AUB

ALIANE Merouane
Directeur Général

Date d'entrée en vigueur : 14/11/2023

MS

Sommaire :

I. Objet
II. Définitions
   1. Système d'Information
   2. Utilisateur
   3. Administrateur
   4. Entité
III. Principes de Sécurité
   1. Protection des informations et des documents électroniques
   2. Protection des moyens et des droits d'accès aux informations
   3. Protection des équipements informatiques
   4. Protection vis-à-vis des échanges sur les réseaux
   5. Protection vis-à-vis de l'accès aux services en ligne sur internet
   6. Publication des Informations sur internet
IV. Vie privée et ressources d'Informatiques personnelles
   1. Vie privée résiduelle
   2. Ressources informatiques personnelles
   3. Gestion des départs
V. Respect de la propriété intellectuelle
VI. Impact des droits et des devoirs spécifiques aux Administrateurs sur les données d'utilisateur
VII. Droits et devoirs d'information
   1. Les obligations de l'Utilisateur
   2. Les obligations d'AUB
VIII. Dispositions de contrôle
IX. Inobservance des règles de la Charte d'utilisation du SI
   1. Mesures d'urgence
   2. Mesures donnant lieu à information
   3. Mesures disciplinaires
X. Révision de la Charte d'utilisation du Système d'information
XI. Formulaire d'engagement
XII. Annexe

Algerian Union Bank Direction Générale

MS

Glossaire :

AUB	Algerian Union Bank
DCH	Direction Capitale Humain
DSI	Direction des Systèmes d'Information
PGSSI	Politique Générale de Sécurité du Système d'Information
RSSI	Responsable Sécurité des Système d'Information
SI	Système d'Information

Algerian Union Bank Direction Générale

Objet

La présente Charte a pour objet d'informer les utilisateurs de leurs droits et de leurs responsabilités, dans le cadre de l'usage des ressources informatiques d'AUB, en application de sa politique générale de sécurité des systèmes d'information, conformément à la règlementation en vigueur.

Elle définit les règles d'usage et de sécurité que l'AUB et les utilisateurs de son Système d'Information doivent respecter et précise les droits et les devoirs de chacun.

Elle répond à la préoccupation de AUB de protéger ses Systèmes d'Information contre toute altération, volontaire ou accidentelle, de leur confidentialité, de leur intégrité ou de leur disponibilité. En effet, tout manquement aux règles qui régissent la sécurité des systèmes d'information est susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux et atteint au bon fonctionnement de la Banque).

II. Définitions

1. Système d'Information

Le terme "Système d'Information" désigne un ensemble organisé de ressources (personnel, matériels, logiciels, données et procédures) qui permet de collecter, de regrouper, de classifier, de diffuser de l'information dans un environnement donné.

2. Utilisateur

Le terme « Utilisateur » (SI) désigne toute personne ayant accès aux ressources des Systèmes d'Information de AUB. Il s'agit, notamment :

- Du personnel d'AUB.
- De toute personne agissant dans le cadre d'une convention, d'un contrat ou d'une relation de partenariat, contractualisée ou non avec AUB.

3. Administrateur

Le terme « Administrateur » fait référence aux utilisateurs, clairement identifiés (privilèges supérieurs sur le SI), en charge de veiller à la sécurité et au bon fonctionnement du Système d'Information.

4. Entité

On désignera sous le terme « entité », toutes les structures crées par AUB pour l'accomplissement de leurs missions, telles que les structures centrales et agences.

III. Principes de sécurité

Les règles ci-après s'appliquent à tout utilisateur et peuvent être complétées par des mesures spécifiques à leur entité résultant de PGSSI opérationnelle.

1. Protection des informations et des documents électroniques

Tout utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès.

Direction Générale

L'utilisateur protège les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité.

Lorsqu'il crée un document, l'utilisateur détermine son niveau de sensibilité et applique les règles permettant de garantir sa protection durant tout son cycle de vie (marquage, stockage, transmission, impression, suppression, etc.).

Lorsque ses données ne font pas l'objet de sauvegarde automatiques mise en place par l'Entité dont il relève, l'utilisateur met en œuvre le système de sauvegarde manuel préconisé par son entité.

Afin de se prémunir contre les risques de vol de documents sensibles, l'utilisateur, lorsqu'il s'absente de son bureau, s'assure que ses documents papier, lorsqu'ils existent, sont rangés sous clé et que son poste de travail est verrouillé.

2. Protection des moyens et des droits d'accès aux informations

L'utilisateur est responsable de l'utilisation des Systèmes d'Information réalisée avec ses droits d'accès.

A ce titre, il assure la protection des moyens d'authentification qui lui ont été affecté ou qu'il a générés (badges, mots de passe, clés privées, clés privées liées aux certificats, etc.) :

- ✓ Il ne les communique jamais, y compris à son responsable hiérarchique et à l'équipe chargée des SI de son Entité ;
- ✓ Il applique les règles de « génération/complexité » et de renouvellement en vigueur selon le moyen d'authentification utilisé ;
- ✓ Il met en place tous les moyens mis à sa disposition pour éviter la divulgation de ses moyens d'authentification ;
- ✓ Il modifie ou demande le renouvellement de ses moyens d'authentification dès lors qu'il en suspecte la divulgation ;
- ✓ Il garantit l'accès à ses données professionnelles, notamment dans le cadre de la politique de recouvrement de données mise en œuvre au sein de l'entité.

L'utilisateur ne fait pas usage des moyens d'authentification ou des droits d'accès d'une tierce personne. De la même façon, il n'essaie pas de masquer sa propre identité.

L'utilisateur ne fait usage de ses droits d'accès que pour accéder à des informations ou à des services nécessaires à l'exercice des missions qui lui ont été confiées et pour lesquels il est autorisé, et de ce fait :

- ✓ Il s'interdit d'accéder ou de tenter d'accéder à des ressources du Système d'Information pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ✓ Il ne connecte pas aux réseaux locaux de l'entité, quelle que soit la nature de ces réseaux (filaires ou non filaires), des matériels autres que ceux confiés ou autorisés par sa Direction ou entité ;
- ✓ Il n'introduit pas des supports de données (clés USB, CDROM, DVD, etc.) sans respecter les règles de l'Entité et prend les précautions nécessaires pour s'assurer de leur innocuité ;
- ✓ Il n'installe pas, ne télécharge pas ou n'utilise pas, sur le matériel de l'entité ou sur du matériel personnel utilisé à des fins professionnelles, des logiciels dont les droits

Direction Générale

de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou interdits par l'entité ;

- ✓ Il s'engage à ne pas apporter, volontairement, des perturbations au bon fonctionnement des ressources informatiques et des réseaux par des manipulations anormales ou matériel ou du logiciel ;

Les responsables hiérarchiques de l'utilisateur informent les Administrateurs, via le Responsable des Ressources Humaines, de toute évolution de ses fonctions nécessitant une modification de ses droits d'accès.

3. Protection des équipements informatiques

L'utilisateur protège les équipements mis à sa disposition :

- ✓ Il applique les consignes issues de PGSSI afin de s'assurer notamment que la configuration de son équipement suit les bonnes pratiques de sécurité, application des correctifs de sécurité, chiffrement, etc ;
- ✓ Il utilise les moyens de protection disponibles (rangement dans un tiroir ou une armoire ferme à clé) pour garantir la protection des équipements mobiles et des informations qu'ils referment (ordinateur portable, clé USB, smartphones, tablettes, etc.) contre le vol ;
- ✓ En cas d'absence, même momentanée, il verrouille ou ferme toutes sessions en cours sur son poste de travail ;
- ✓ Il signale, le plus rapidement possible, au RSSI toute perte, vol ou toute compromission suspectée ou avérée d'un équipement mis à sa disposition.

L'utilisateur protège les équipements personnels qu'il utilise pour accéder, à distance ou à partir du réseau local d'une entité, aux SI d'AUB ou pour stocker des données professionnelles en respectant les règles édictées par AUB et par l'entité.

L'Entité informe l'Utilisateur et l'accompagne dans la mise en œuvre de ses mesures de protection.

4. Protection vis-à-vis des échanges sur les réseaux

4.1. Adresse Electronique

La messagerie électronique d'AUB est un moyen de communication principalement professionnel. Toutefois, il peut être toléré un usage privé et ce, à titre subsidiaire, dans ce cas, l'Utilisateur doit s'abstenir de transmettre des fichiers susceptibles de réduire les performances de la bande passante.

Aussi, tout utilisateur ayant accès aux ressources du système d'information, est doté d'une adresse de messagerie du domaine d'AUB, dont l'usage est placé sous sa responsabilité.

L'utilisateur doit consulter, régulièrement, sa boite de messagerie. En cas d'absence prévue et prolongée, il doit le signaler au niveau du menu correspondant dans Outlook ou autre email autorisé par la Banque, en mentionnant la durée et le motif de cette absence.

Les courriels transmis ou reçus via la messagerie électronique du domaine d'AUB, sont considérés comme des documents officiels au sein de la Banque.

Algerian Union Bank — Direction Générale — AUB

La messagerie électronique d'AUB ne doit en aucun cas être utilisée pour l'inscription dans des sites ou des forums sur le WEB en dehors du périmètre tracé par la politique de sécurité.

La messagerie électronique peut connaitre des limitations en termes de messages entrants ou sortants, compte tenu des impératifs de sécurité du SI. Dans ce cadre, les messages privés à caractère de diffusion multiple ou générale, sont totalement proscrits.

Les messages peuvent constituer une preuve opposable à l'utilisateur, ce dernier doit porter tout le soin au contenu des messages qu'il échange dans un cadre professionnel ou personnel.

4.2. Contenu des échanges sur les réseaux

Les échange électroniques (courriels, forums de discussion, messagerie instantanée, réseaux sociaux, partage de documents, voix, images, vidéos, etc.) doivent respecter la correction normalement attendue dans tout type d'échange tant écrit qu'oral.

La transmission de données classifiées de secret défense est interdite sauf dispositif spécifique agréé et la transmission de données sensibles doit être réalisée suivant les règles de protection en vigueur.

4.3. Vigilance

Les informations font preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage,….).

4.4. Statut et valeur juridique des informations échangées

Les informations échangées, par voie électronique, avec des tiers peuvent, au plan juridique, former un contrat sous certaines conditions ou encore être utilisées à des fins probatoires.

L'utilisateur doit, en conséquence, être prudent sur la nature des informations qu'il échange par voie électronique au même titre que pour les courriers traditionnels.

4.5. Stockage et archivage des informations échangées

L'utilisateur est informé que le courriel est un document administratif reconnu en tant que preuve en cas de contentieux.

5. Protection vis-à-vis de l'accès aux services en ligne

Si une utilisation à caractère privée peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique, mis à disposition par AUB sont considérées comme professionnelles.

L'utilisateur utilise ses codes d'accès, en particulier son adresse électronique ou autre identifiant, avec précaution. En les utilisant sur des sites sans rapport avec son activité professionnelle, il facilite les atteintes à sa réputation, à la réputation de l'entité et à celle d'AUB.

Certains sites malveillants profitent des failles des navigateurs pour récupérer les données présentes sur le poste de travail. D'autres sites mettent à disposition des logiciels qui, sous une apparence anodine, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu au pirate à l'insu de l'utilisateur. Enfin, certains sites ne fournissent aucune garantie sur l'utilisation ultérieure qui pourra être faite des données transmises.

Par conséquent, l'utilisateur doit :

- Eviter de se connecter à des sites suspects ;
- Eviter de télécharger des logiciels dont l'innocuité n'est pas garantie (nature de l'éditeur, mode de téléchargement, etc.) ;
- Ne pas opérer les sauvegardes de données, les partages d'information, les échanges collaboratifs que sur des sites de confiance, mis à disposition par l'établissement, et dont la sécurité a été vérifiée (via par exemple un audit de sécurité) ;
- Chiffrer les données non publiques qui seraient stockées sur des sites tiers ou transmis via des messageries non sécurisées.

La DSI se réserve le droit d'interdire l'accès à certains sites pouvant être considérés comme contraires à l'esprit et à la lettre de politique générale de sécurité informatique de la Banque.

La DSI se réserve, également le droit de procéder à des contrôles à priori et à postériori des accès aux sites ainsi que le temps de consultation desdits sites. Elle peut, par la suite, et si elle le juge nécessaire, limiter ou interdire l'accès aux utilisateurs et/ou dits sites.

6. Publication d'informations sur internet

Toute publication d'informations sur les sites internet ou intranet de l'entité est réalisée sous la responsabilité d'un responsable de site ou responsable de publication nommément désigné.

Aucune publication d'informations à caractère privé (pages privées au sens non professionnelles) sur les ressources du système d'information de l'entité n'est autorisée, sauf disposition particulière décidée au sein de l'entité.

IV. Vie privée et ressources informatiques personnelles

1. Vie privée résiduelle

Vie privée et ressources informatiques (postes de travail, serveurs, applications, messagerie, internet, téléphones, etc.) fournies à l'utilisateur, par AUB ou ses partenaires, sont réservées à l'exercice de son activité professionnelle.

Un usage personnel de ces ressources est toutefois toléré à condition :

- ✓ Qu'il reste de courte durée pendant les heures de travail au bureau ;
- ✓ Qu'il n'affecte pas l'usage professionnel ;
- ✓ Qu'il ne mette pas en danger le bon fonctionnement et la sécurité des équipements et des ressources ;
- ✓ Qu'il n'enfreigne pas la loi, les règlements et les dispositions internes ;
- ✓ Qu'il soit non lucratif, raisonnable et n'occasionne pas de surcoûts considérables pour la Banque.

Toute donnée est réputée professionnelle à l'exception des données explicitement désignées par l'utilisateur comme ayant un caractère privé (par exemple en indiquant la mention "privé" dans le champ « objet » des messages).

L'utilisateur procède au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource utilisée. Cet espace ne doit pas contenir de données à caractère professionnel et il ne doit pas

Direction Générale

occuper une part excessive des ressources. La protection et la sauvegarde régulière des données à caractère privé incombent à l'utilisateur.

La diffusion d'idéologies politiques ou religieuses, ou qui sont de nature à porter atteinte à l'image de la Banque et aux bonnes mœurs, à la dignité, à l'honneur, ou à la vie privée de personnes physiques sont interdites.

2. Ressources informatiques personnelles

Les ressources informatiques personnelles (ordinateurs, smartphones, tablettes, etc.) acquis à titre personnel, lorsqu'elles sont utilisées pour accéder aux SI d'AUB, ne doivent pas remettre en cause ou affaiblir, les politiques de sécurité en vigueur dans les entités par une protection insuffisante ou une utilisation inappropriée. Lorsque ces ressources informatiques personnelles sont utilisées pour accéder, à distance ou à partir d'un réseau local d'une entité, aux SI d'AUB ou pour stocker des données professionnelles, ces ressources sont autorisées et sécurisées suivant les directives issues de la PGSSI et déclarées au service informatique qui gère le parc matériel de l'entité.

Le personnel qui souhaiterait faire l'acquisition de tels matériels prend, préalablement conseil auprès du service informatique.

3. Gestion des départs

L'utilisateur est responsable de son espace de données à caractère privé et il lui appartient de le détruire au moment de son départ. En cas des circonstances exceptionnelles (départ impromptu ou décès) AUB ne conserve pas les espaces de données à caractère privé présents sur les ressources informatiques fournis par AUB que pour une période maximale de trois (03) mois (délais permettant à l'utilisateur ou ses ayant droits de récupérer les informations qui s'y trouvent).

Les données professionnelles restent à la disposition de l'employeur. Les mesures de conservation des données professionnelles sont définies au sein de l'entité.

Dès le départ de l'utilisateur, son responsable hiérarchique doit prévenir l'Administrateur système pour suspendre les accès aux courriels et aux données du système d'information.

V. Respect de la propriété intellectuelle

L'utilisateur ne reproduit pas, ne télécharge pas, ne copie pas, ne diffuse pas, ne modifie pas, n'utilise pas les logiciels, les bases de données, les pages web, les images, les photographies ou autre créations protégées par les droits d'auteur ou un droit privatif, sans avoir obtenu, préalablement, l'autorisation des titulaires de ces droits.

VI. Impact des droits et des devoirs spécifiques aux administrateurs sur les données des utilisateurs

L'administrateur à accès aux traces (ou logs) laissées par l'utilisateur lors de ses accès sur l'ensemble des ressources informatiques mises à sa disposition par l'entité ainsi que sur les réseaux locaux et distants.

Les administrateurs peuvent, en cas de dysfonctionnement technique, d'intrusion ou de tentative d'attaque sur les systèmes informatiques, utiliser ces traces pour tenter de trouver l'origine du problème.

A ce titre, ils sont soumis à une obligation de confidentialité. Ils peuvent donc divulguer les informations qu'ils sont amenés à connaitre dans le cadre de leur fonction, en particulier l'lorsqu'elles couverts par le secret des correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent pas en cause ni le bon fonctionnement technique des applications, ni leur sécurité.

Ils ne peuvent prendre connaissance du contenu des répertoires, des fichiers ou des messages, manifestement et explicitement désignés comme personnels, qu'en présence de l'utilisateur et avec son autorisation expresse, et cela pour les cas d'urgences justifiées ou de nécessité vis-à-vis de la législation et de la sécurité

VII. Droits et devoirs d'information

AUB s'oblige à porter, à la connaissance de l'ensemble des utilisateurs du système d'information, le contenu de la présente charte.

L'utilisateur s'engage, à porter à la connaissance de l'administrateur, tout dysfonctionnement ou anomalie touchant le système d'information au sens de la présente charte.

1. Les obligations de l'utilisateur

L'utilisateur contribue, à son niveau, à la sécurité des Systèmes d'Information, il s'engage notamment à :

- Respecter les lois et règlements en vigueur ;
- Respecter la présente Charte ;
- Prendre soin des matériels, des logiciels et des locaux mis à sa disposition ;
- Faire une utilisation non abusive des moyens informatiques auxquels il a accès ;
- Respecter les mesures de sécurité mises en place ;
- Se conformer aux décisions des responsables informatiques ;
- Ne pas utiliser ou tenter d'utiliser le compte d'un tiers ;
- Veiller à la confidentialité des codes, des mots de passe ou tout autre dispositif de contrôle d'accès qui lui confié ;
- Signaler, sans délai, tout dysfonctionnement ou incident de sécurité potentiel ;
- Veiller à ce que les données confidentielles à l'égard des informations et des documents auxquels il accède ;
- Respecter les droits d'auteur et les licences d'utilisation.

2. Les obligations d'AUB

AUB s'engage à :

- Respecter les lois et les règlements en vigueur ;
- Assurer le bon fonctionnement et la disponibilité des services numériques ;
- Maintenir la qualité du service fourni, dans la limite des moyens alloués ;
- Informer les usagers des règles et des bons usages tels qu'ils sont définis dans la présente Charte et dans la Politiques Générale de Sécurité Informatique ;
- Veiller à respecter la confidentialité des correspondances électroniques et des fichiers auxquels son personnel a accès dans le cadre de son activité ;
- Veiller à la bonne utilisation des systèmes d'information, notamment :
  - ✓ En prenant toutes mesures nécessaires pour assurer ou préserver le bon fonctionnement et/ou la disponibilité nominales des moyens informatiques ;

Direction Générale

- ✓ En conservant, temporairement, les journaux sur l'activité des réseaux et des systèmes, qui font par ailleurs l'objet d'une surveillance automatisée ;
- Assurer la sécurité des ressources exploitées par le personnel ;
- Favoriser l'instauration d'une culture « Sécurité ».

VIII. Dispositions de contrôle

L'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau, peuvent être analysés, contrôlés voire filtrés par la DSI.

La DSI est investie du droit de fournir la traçabilité quant à l'utilisation des ressources, au Responsable de la Sécurité des Systèmes d'Information, suite à la demande de ce dernier, sans pour autant avoir l'obligation d'en aviser l'utilisateur.

Le Responsable de la Sécurité des Systèmes d'Information, dans le cadre de ses missions réserve le droit de :

- Contrôler l'utilisation par les administrateurs des ressources mises à disposition, à des fins d'audit, de sécurité, de traçabilité et afin de prévenir tout usage abusif ou contraire aux prescriptions sus énoncées. Toutefois, ce contrôle demeure du ressort exclusif des personnes désignées et habilitées ;
- Contrôler la bonne exécution des règles de sécurité destinées aux Administrateurs.

La DSI, dans le cadre de la conduite de la Politique Générale de Sécurité Informatique, se réserve le droit de :

- Effectuer toute forme de maintenance corrective ou évolutive sur le système d'information, sans requérir l'aval de l'utilisateur. Toutefois, ce dernier serait informé par voie électronique ;
- Procéder à toute intervention à distance entrant dans le cadre de maintenance telle que définie ci-haut, ainsi que de procéder à toute action tendant à prévenir, à limiter ou à traiter toute forme de menace pouvant toucher le Système d'Information.

La Direction Gestion des Risques et la Direction de l'Audit Interne sont les organes de contrôle chargés de veiller au respect des dispositions de la présente Charte, chacun dans le cadre de ses missions et des procédures propres aux dites fonctions.

IX. Inobservance des règles de Charte d'utilisation du SI

Le manquement aux règles et aux mesures de sécurité et de confidentialité définies par la présente Charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

Le non-respect des lois et des textes applicables en matière de sécurité des Systèmes d'Information est susceptible de sanctions pénales prévues par la loi.

Tout manquement aux dispositions de la présente Charte, selon le degré de gravité, pourrait conduire à une suspension temporaire ou définitive de l'accès aux ressources du Système d'Information.

Tout manquement aux dispositions de la présente Charte, selon le niveau de gravité, pourrait conduire aux sanctions suivantes :

Algerian Union Bank Direction Générale

1. Mesure d'urgence

AUB, peut en cas d'urgence, prendre toute mesure pour arrêter la perturbation de ses services informatiques, tel que :

- ✓ Déconnecter un utilisateur, avec ou sans préavis, selon la gravité de la situation ;
- ✓ Isoler ou neutraliser toute donnée qui mettrait en péril les moyens informatiques ou qui serait en contradiction avec cette Charte.

2. Mesures donnant lieu à information

En cas de non-respect de cette Charte par l'utilisateur, AUB :

- ✓ Prend contact avec l'utilisateur et/ou son responsable hiérarchique ;
- ✓ Procéder à la suppression temporaire ou définitive de l'accès aux ressources du Système d'Information.

3. Mesures disciplinaires

Les manquements jugés attentatoires à la Sécurité des Systèmes d'Information et pouvant avoir des répercussions préjudiciables pour AUB, peuvent être passible à de sanctions disciplinaires et/ou judiciaires suivant la qualification de la faute professionnelle du dit manquement conformément aux dispositions ou Règlement Intérieur et du Code de Déontologie d'AUB.

X. Révision de Charte d'utilisation du Système d'Information

Cette Charte est susceptible d'être modifiée à chaque fois que l'usage des ressources informatiques et/ou les évolutions technologiques l'imposent.

L'utilisateur s'engage au respect de l'ensemble des dispositions de la présente Charte, y compris ses éventuelles futures modifications et/ou mises à jour.

XI. Formulaire d'engagement

Le formulaire d'engagement joint en annexe à cette Charte doit être, dûment, renseigné et signé, par l'ensemble du personnel d'AUB ayant accès au Système d'Information de la Banque.

A ce titre, chaque responsable de structure aura à transmettre le dit formulaire, à la Direction du Capital Humain, aux fins d'être versé et joint au dossier administratif de l'utilisateur concerné.

XIII. Annexe

- Formulaire d'engagement.

Algerian Union Bank — Direction Générale — AUB

MS

Formulaire d'engagement

Je soussigné(e),

Nom :

Nom de jeune fille :

Prénom(s) :

Date et lieu de naissance :

Fonction :

Matricule :

Déclare avoir reçu la Charte d'utilisation du Système d'Information d'AUB et avoir pris connaissance de son contenu. Je m'engage à respecter l'ensemble de ses dispositions, y compris ses éventuelles futures modifications et/ou mises à jour.

Date :

Signature

NB :
Ce formulaire une fois renseigné et signé par l'utilisateur, fera l'objet de transmission à la DCH.

Algerian Union Bank — Direction Générale — AUB

MS