Directive

GUI-GSI-SSI-012

Consignes de sécurité pour les partenaires V1.0

C0 : Public

Contenu

0. Préface

0.1. Objet du présent document

Les règles de sécurité de l'information, auxquelles les fournisseurs de services doivent se conformer lorsqu'ils traitent des informations et utilisent du matériel informatique, sont fournies dans la présente ligne directrice sur la sécurité de l'information.

Prestataire de services désigne tout tiers qui fournit un service à ALTEN sur la base d'une relation contractuelle.

Ces directives de sécurité sont destinées à la direction de la société prestataire de services, à ses employés et à ses agents d'exécution /agents (ci-après dénommés le contractant).

0.2. Portée

Ces directives s'appliquent à tous les prestataires de services qui fournissent des services à Alten Delivery Center Maroc conformément aux accords contractuels.

0.3. Structure du document

Chapitre	Groupe-cible	Commentaires
1	Tous les fournisseurs de services	Tous les fournisseurs de services sont tenus de se conformer aux exigences énoncées dans le présent chapitre. Des exigences supplémentaires sont énoncées aux chapitres 2 et 3. Ils exigent une conformité en fonction des possibilités d'accès au réseau de l'entreprise et aux systèmes de l'entreprise.
2	Prestataires de services ayant accès au réseau de l'entreprise ou aux systèmes de l'entreprise	En outre, les exigences du chapitre 1 doivent être respectées. Si le fournisseur de services a accès au réseau client et aux systèmes du client, il doit également suivre les directives du client.
3	Fournisseurs de services sans accès au réseau ou aux systèmes de l'entreprise	En outre, les exigences du chapitre 1 doivent être respectées.

1. Exigences générales

Les exigences suivantes doivent être respectées par tous les fournisseurs de services, conformément à la définition fournie dans le présent document.

Les exigences pour le Client ne font pas partie de ce document.

1.1. Exigences organisationnelles

Toute règle du Client relative à l'apport de matériel informatique n'appartenant pas au Client dans les locaux de l'entreprise ou dans des zones de sécurité restreinte (bureaux de projet) doit être respectée.

La divulgation de données à des tiers n'est autorisée qu'avec l'accord écrit du propriétaire des données du Client.

Toutes les règles du Client relatives à l'utilisation, au stockage et à tout type de traitement des données personnelles (voir également Annexe A.1.2) doivent être respectées.

Les employés du prestataire de services doivent être tenus par la direction de maintenir la confidentialité au sens de l'accord de confidentialité existant entre le client et le contractant. Le Client doit être autorisé à consulter ces accords à tout moment.

Si les données des clients doivent être stockées sur des systèmes mobiles ou des équipements informatiques, elles doivent être cryptées avec du matériel ou des logiciels de pointe.

Lors de la résiliation du contrat, les données du client doivent être remises au client et doivent être effacées sur l'équipement et les supports de stockage du fournisseur de services. Les spécifications du Client et toutes les exigences légales (par exemple, accord de confidentialité, accord-cadre, obligations de conservation) doivent être respectées.

1.2. Sécurité personnelle

Un identifiant d'utilisateur ou une autorisation d'accès aux données du client qui ne sont plus nécessaires doit être signalé sans délai par l'utilisateur au bureau de mise en service concerné (par exemple, administrateur de l'utilisateur).support informatique responsable ou client, voir A.1.4), afin que le blocage et l'effacement nécessaires puissent être effectués.

Les supports d'identification qui ne sont plus nécessaires (par exemple, les jetons RSA) doivent être retournés sans délai au bureau de mise en service.

Tout équipement (par exemple, ordinateurs portables) et supports de données ou supports de stockage fournis doit être retourné au client à l'expiration de l'accord ou lorsqu'ils ne sont plus nécessaires.

La perte du matériel informatique fourni à l'utilisateur et des supports à des fins d'authentification doit être notifiée par l'utilisateur au bureau compétent du Client (voir Annexe A.1.4).

1.3. Sécurité physique et environnementale

Les équipements informatiques qui stockent ou traitent les données des clients doivent être utilisés de manière à ce que les personnes non autorisées ne puissent pas les consulter ou y accéder. Une attention particulière est requise lors de l'utilisation de systèmes mobiles.

Les documents confidentiels et secrets ne doivent jamais être laissés sans surveillance, afin d'empêcher les personnes non autorisées de les consulter.

1.4. Gestion des valeurs internes

1.4.1. Règles de classification

La classification est effectuée sur la base des trois objectifs de protection que sont la confidentialité, l'intégrité et la disponibilité, et doit être mise en œuvre pour toutes les informations et tous les systèmes informatiques de traitement de l'information.

Le but de cette classification est d'attribuer un niveau à l'information, quels que soient les besoins de protection. Différentes mesures de protection seront nécessaires en fonction de cette classification.

Les informations (objectif de protection confidentiel) doivent être protégées contre l'accès par des personnes non autorisées pendant toute la durée de leur vie, conformément aux mesures relatives à leur classification de confidentialité. Lors du traitement des données, la classification par rapport à l'intégrité et à la disponibilité devrait être déterminée par le propriétaire du processus, si nécessaire. Cette classification devrait être régulièrement évaluée avec la participation du propriétaire de l'information et, le cas échéant, révisée.

1.4.1.1 Confidentialité

Les informations qui ne sont pas destinées au grand public ne doivent être rendues accessibles qu'aux personnes autorisées à y accéder (principe : sur la base du « besoin d'en connaître »).

Spécifications pour l'auteur et le propriétaire de l'information :

- Les nouvelles informations et données doivent être étiquetées par l'auteur.
- Le propriétaire de l'information est responsable de la classification.
- L'auteur doit demander la classification correcte au propriétaire des informations.
- Tous les systèmes informatiques doivent être affectés à un niveau de classification de confidentialité.
- Lorsqu'un niveau de classification n'est pas sans ambiguïté, par exemple, dans le cas de documents/systèmes informatiques nouvellement saisis, le niveau « confidentiel » doit être sélectionné.
- Le propriétaire des informations doit (au plus tard lors de la prochaine révision ou mise à jour) vérifier si la classification de confiance des informations internes (C1), confidentielles (C2) et strictement confidentielles (C3) est toujours correcte et l'étiqueter en conséquence.

Spécifications pour le destinataire :

- Les informations et données non marquées sont considérées comme confidentielles.
- En cas de doute sur la classification, contactez le propriétaire des informations.

Les niveaux de classification suivants sont définis en fonction de la confidentialité de l'information :

Classification	Définition
Public (C0)	Cela concerne toutes les informations qui ont été publiées par ALTEN et qui sont donc librement accessibles, telles que : • Matériel publicitaire (dépliants, etc.) • Tous les espaces publics sur le site Dans le cas de matériel publicitaire (dépliants, etc.), les informations ne doivent pas être étiquetées.
Interne (C1)	Cela concerne toutes les informations dont la divulgation involontaire ou leur divulgation à un tiers peut causer un préjudice à l'entreprise. Cela comprend généralement des informations accessibles par un plus grand groupe d'employés, mais pas par des parties externes, telles que : • Communication interne (correspondance par email, équipes virtuelles), • Règles et règlements internes (lignes directrices, mémos, instructions ou tableaux d'organisation), • Information interne (résultats du travail, plans et intentions), • Publications sur l'intranet

Confidentiel (C2)	Il s'agit de toutes les informations dont la divulgation involontaire ou la divulgation à un tiers peut causer un préjudice financier considérable à ALTEN, peut avoir des conséquences juridiques ou nuire à la réputation d'ALTEN. Ces informations doivent toujours être étiquetées « confidentielles ». Cela inclut généralement toutes les informations qui sont significatives pour la réussite technique ou financière de chaque département. Cela inclut en particulier toutes les informations qui pourraient être d'une valeur particulière pour les concurrents, telles que : • Communications confidentielles (correspondance client par courriel, vidéo-conférence et collaboration), • Assurer la compétitivité (données marketing, données clients et fournisseurs, requêtes clients), • Données personnelles, • Frais de déplacement et bulletins de salaire, • Données de recherche, • Information sur les projets (commerciaux, techniques), • Données techniques (dessins de construction de zones sensibles, plans de réseau)
Strictement confidentiel (C3)	Il s'agit d'informations commerciales confidentielles dont la divulgation involontaire ou la divulgation à un tiers peut entraîner un préjudice grave à l'objet et aux objectifs commerciaux d'ALTEN, des conséquences juridiques graves ou des dommages graves à la réputation d'ALTEN. Ce type d'information doit toujours être étiqueté avec la classe de protection « strictement confidentielle ». Cela inclut généralement des informations extrêmement importantes pour le succès et la pérennité de l'ensemble de l'entreprise, telles que : • Stratégies d'entreprise, • Planification technique et stratégique, • Informations sur les acquisitions ou les investissements d'entreprises prévus, • Plans économiques et budgétaires de différents départements, • Informations provenant de partenaires commerciaux ayant le même niveau de confidentialité, • Informations sur les situations de crise, • Copies d'informations strictement confidentielles

1.4.1.2 Intégrité

Le traitement sans erreur des informations et la protection contre les révisions non autorisées doivent être assurés. Les niveaux de classification suivants sont définis en fonction de l'intégrité de l'information :

Classification	Définition
Bas	Une atteinte à l'intégrité n'a pas d'effets prévisibles sur les activités commerciales ou l'image ou l'apparence de l'entreprise.
Douleur moyenne	Une atteinte à l'intégrité n'a qu'un impact mineur sur les activités commerciales et/ou l'image ou l'apparence de l'entreprise. Il peut y avoir des conséquences négatives, même dans une mesure limitée. Exemples : • Petits retards avec les processus de flux de travail • Erreurs qui n'ont pas d'impact sur les résultats du travail (pas de temps d'arrêt productifs) • Les décisions ne sont pas affectées • Les demandes de dommages et intérêts par des individus ou des organisations sont peu probables
Haut	Une atteinte à l'intégrité a un effet notable sur les activités commerciales et/ou l'image ou l'apparence de l'entreprise. Il est probable qu'il y aura des conséquences négatives mesurables, par exemple : • La perte de clients est probable • Effacer les retards dans les processus de flux de travail • Erreurs/dysfonctionnements ayant des effets perceptibles sur les résultats du travail (niveau élevé d'indisponibilité de la production) et/ou perturbation de certains processus de service • Les décisions sont influencées / les décisions incorrectes sont probables • Les demandes de dommages et intérêts par des individus ou des organisations sont probables
Très élevé	Une atteinte à l'intégrité a un effet considérable sur les activités commerciales et/ou l'image ou l'apparence de l'entreprise et les conséquences correspondantes, par exemple : • Perte importante de clients • Les demandes de dommages et intérêts par des individus ou des organisations sont peu probables • Exclusion de certaines régions de marché • Effacer les retards dans les processus de flux de travail • Erreurs/dysfonctionnements ayant un effet grave sur les résultats du travail et/ou perturbation d'un certain nombre de processus de service (niveau très élevé de temps d'arrêt de production) • Les décisions sont fortement affectées / des décisions incorrectes sont prises Exemples : Comptabilité (p. ex. rapport annuel), brevets, clés cryptographiques, relevés de salaire

1.4.1.3 Disponibilité

Les informations doivent être disponibles dans un délai convenu.

Les classifications suivantes ont été définies en fonction de la disponibilité de l'information :

Classification	Définition
Bas	La disponibilité du système informatique en termes de perturbation ou de temps de réponse inacceptables peut être inférieure à 95%, sans que cela n'entraîne une dépréciation significative (par exemple de nature financière ou pour l'image de l'entreprise).
Douleur moyenne	La disponibilité du système informatique en termes de perturbation ou de temps de réponse inacceptables doit être d'au moins 95%. Un niveau de disponibilité inférieur entraînera une dépréciation importante (par exemple, de nature financière ou de l'image de l'entreprise).
Haut	La disponibilité du système informatique en termes de perturbation ou de temps de réponse inacceptables doit être d'au moins 98 %. Un niveau de disponibilité inférieur entraînera une dépréciation importante (par exemple, de nature financière ou de l'image de l'entreprise).
Très élevé	La disponibilité du système informatique en termes de perturbation ou de temps de réponse inacceptables doit être d'au moins 99%. Un niveau de disponibilité inférieur entraînera une dépréciation importante (par exemple, de nature financière ou de l'image de l'entreprise). Exemple : Lorsque la perturbation d'un système informatique entraîne un arrêt immédiat de la production Une déficience importante peut être, par exemple : • Perte de clients • Demandes de dommages et intérêts de diverses personnes, organisations ou associations Erreurs/dysfonctionnements ayant un effet grave sur les résultats du travail et/ou perturbation de plusieurs processus de service (temps d'arrêt de production très élevés)

1.4.2. Informations sur l'étiquetage et le traitement

Les informations ne peuvent être rendues accessibles à un groupe de personnes autorisées qu'aux fins des activités convenues et conformément à la réglementation applicable. Le principe du « besoin de savoir» doit être respecté ici.

Les informations doivent être protégées contre l'accès par des personnes non autorisées pendant toute la durée de leur vie, conformément à leur classification de confidentialité actuelle. Les lignes directrices suivantes s'appliquent :

Classification	Exigences
Public	Les spécifications internes de l'entreprise sur la position de l'étiquette de classification s'appliquent : • Label : « Public » (possibilité de se passer d'étiquette sur les flyers ou d'autres mesures de marketing) • **Reproduction et distribution :** aucune restriction • **Stockage :** aucune restriction • **Effacement** : aucune restriction • **Élimination** : aucune restriction

Interne (C1)	Les spécifications internes de l'entreprise sur la position de l'étiquette de classification s'appliquent : • **Étiquette :** Détails du niveau de confidentialité dans la langue du pays / « interne » sur chaque page du document en format électronique et imprimé. • **Reproduction et distribution :** uniquement aux employés autorisés de la société et aux tiers autorisés, dans le cadre de l'activité ou du champ d'application. • **Stockage :** Protection contre les accès non autorisés • **Effacement :** Les données qui ne sont plus nécessaires doivent être effacées (voir l'annexe A.1.2, A.1.3) • **Élimination :** élimination appropriée (voir annexe, A.1.2, A.1.3)
Confidentiel (C2)	Les spécifications internes de l'entreprise sur la position de l'étiquette de classification s'appliquent : • **Étiquette :** Détails du niveau de confidentialité dans la langue du pays / « Confidentiel » sur chaque page du document en format électronique et imprimé. • **Reproduction et distribution :** uniquement à un groupe limité d'employés autorisés de la société et de tiers autorisés dans le cadre de l'activité et du champ d'application. La personne qui distribue les informations est responsable de la recherche de canaux de distribution utilisables afin de protéger les informations et les données contre tout accès non autorisé et/ou toute écoute non autorisée (par exemple, en utilisant le cryptage). • **Stockage :** Accès uniquement pour un groupe limité d'employés autorisés de l'entreprise et de tiers autorisés dans le cadre de l'activité et du champ d'application (par exemple au moyen d'un groupe d'utilisateurs fermé). Des emplacements de stockage et/ou des supports de stockage appropriés doivent être utilisés. • **Effacement :** les données qui ne sont plus nécessaires doivent être effacées (voir appendice x A.1.2, A.1.3) • **Élimination :** élimination appropriée (voir annexe, A.1.2, A.1.3) • **Authentification :** Authentification forte (2e facteur) • **Transport :** Les documents confidentiels et les supports de stockage doivent être expédiés dans des enveloppes scellées et neutres; si nécessaire, le mot « personnel » peut être ajouté. Cela signifie que l'enveloppe ne peut être remise directement qu'au destinataire désigné .

Strictement confidentiel (C3)	Les spécifications internes de l'entreprise sur la position de l'étiquette de classification s'appliquent : • **Étiquette :** Détails du niveau de confidentialité dans la langue du pays / « Strictement confidentiel » sur chaque page du document en format électronique et imprimé. De plus, toutes les pages doivent inclure le texte « page x de y ». • **Reproduction et distribution :** uniquement pour un groupe extrêmement limité (par exemple, liste de noms) d'employés autorisés de l'entreprise et de tiers autorisés dans le cadre de l'activité ou du champ d'application et après accord préalable du propriétaire de l'information. Lorsque cela est techniquement possible, toutes les données doivent être cryptées conformément à l'état de la technique. Lorsque cela n'est pas possible, des solutions de sécurité d'une puissance comparable doivent être utilisées. Selon le type d'application, d'autres mesures de protection techniques ou organisationnelles doivent être prises (par exemple, interdiction d'expédition et d'impression, filigrane) • **Pour la communication :** des supports appropriés doivent être utilisés pour empêcher les écoutes (par exemple, vidéo-conférences cryptées). • **Stockage :** Accès uniquement pour un groupe extrêmement limité (par exemple, liste de noms) d'employés autorisés de l'entreprise et de tiers autorisés dans le cadre de l'activité ou du champ d'application (par exemple, sur la base de groupes d'utilisateurs fermés). Lorsque cela est techniquement possible, toutes les données doivent être cryptées conformément à l'état de la technique. Lorsque cela n'est pas possible, de manière comparable des solutions de sécurité solides doivent être utilisées. • **Effacement :** Les données qui ne sont plus nécessaires doivent être effacées (voir l'annexe A.1.2, A.1.3) • **Élimination :** élimination appropriée (voir annexe, A.1.2, A.1.3) • **Authentification :** Authentification forte (2e facteur) • **Transport :** Les documents et supports de stockage strictement confidentiels doivent être expédiés dans des enveloppes neutres et scellées (sans ajouter de mots tels que « personnel », « secret », etc.) Une deuxième enveloppe doit être placée à l'intérieur de l'enveloppe, und doit être marqué du niveau de classification « secret » ou « strictement confidentiel ».

Les renseignements non étiquetés qui ne sont manifestement pas « publics » doivent être classés comme « confidentiels ».

Les spécifications relatives au traitement des informations (étiquetage, reproduction, distribution, stockage, effacement et élimination) s'appliquent également aux systèmes informatiques (par exemple, bases de données et supports de sauvegarde).

1.4.3. Gestion des supports de stockage

Les supports de données (tels que les CD, DVD, clés USB et disques durs) doivent être protégés contre la perte, la destruction et la confusion et contre les accès non autorisés.

Les supports de données qui ne sont plus nécessaires doivent être éliminés de manière sécuritaire (voir l'annexe A.1.3).

1.4.3.1 Échange d'informations

Il est important de veiller à ce que toutes les conversations (y compris les appels téléphoniques, les vidéo-conférences et les conférences Web) qui impliquent ou contiennent des informations confidentielles ou secrètes ne puissent pas être entendues sans autorisation.

Afin d'éviter une transmission incorrecte, les répertoires actuels doivent être vérifiés par les numéros de fax et les adresses e-mail ou ceux-ci doivent être vérifiés avec le destinataire.

L'expéditeur est responsable du contenu et de la distribution d'un e-mail. Le destinataire est responsable du traitement et de la distribution ultérieurs.

1.5. Traitement des incidents liés à la sécurité de l'information

Les incidents de sécurité de l'information (par exemple, perturbation, violation de la législation sur la sécurité de l'information), qui concernent les données ou les systèmes du client, doivent être notifiés sans délai au bureau concerné (voir annexe, A.1.4).

Les vulnérabilités et les faiblesses présumées des systèmes informatiques doivent être signalées sans délai au bureau compétent (voir l'annexe A.1.4).

Si l'on soupçonne une perte de renseignements confidentiels ou secrets, elle doit être signalée sans délai au bureau compétent (voir l'annexe A.1.4 et A.1.5).

1.6. Conformité et respect des obligations légales

Le prestataire de services doit mettre en place un système de gestion de la conformité en tenant compte des exigences légales et de l'entreprise (y compris la gestion des ressources, le système de contrôle interne, la gestion de la continuité informatique et la protection des informations). Il doit inclure toutes les informations, le matériel et les logiciels du Client.

Le bureau compétent (voir annexe, A.1.4) doit être contacté en cas de questions et pour obtenir de l'aide.

Le système de gestion de la conformité doit contenir les éléments suivants :

1.6.1. Détection précoce des risques

Un processus de reconnaissance précoce des risques et des menaces potentielles pour les systèmes informatiques et les données doit être mis en œuvre.

Des mesures préventives doivent être prises pour faire face aux risques reconnus.

1.6.2. Propriété intellectuelle / gestion des licences

Tous les droits de propriété intellectuelle (par exemple, les droits d'auteur sur les logiciels, les documents et graphiques, les droits de conception, les marques de commerce, les brevets et les licences de code source) doivent être respectés et respectés.

L'utilisation de logiciels sans licence (copies piratées) n'est pas autorisée.

Pour les logiciels sous licence, les dispositions légales s'appliquent en ce qui concerne le droit d'auteur (par exemple, lorsque la réalisation de copies constitue une violation du droit d'auteur, à l'exception des copies effectuées à des fins de sauvegarde et d'archivage). Une violation de ces dispositions peut entraîner des poursuites pénales et une jonction provisoire ou une demande de dommages-intérêts.

Le logiciel sous licence ne doit être utilisé qu'aux fins convenues et conformément à la législation applicable et aux accords de licence conclus avec le fabricant.

1.6.3. Confidentialité des données

La législation et les dispositions spécifiques à chaque pays en matière de confidentialité des données (voir l'annexe A.1.8) doivent être respectées.

Les contractants doivent être tenus par la direction du fournisseur de services concerné de se conformer à la législation légale sur la confidentialité des données.

1.6.4. Conformité contractuelle

L'organisation informatique du prestataire de services doit répondre aux exigences contractuelles du Client. Des mesures doivent être prises pour s'assurer que les propres règles organisationnelles des prestataires de services sont examinées et tenues à jour, de sorte que les exigences contractuelles actuelles soient incluses.

1.6.5. Instructions internes

Les fournisseurs de services doivent préciser les règlements et le code de conduite à leurs employés afin d'assurer la conformité aux exigences et la conduite appropriée lors du traitement des informations et du matériel et des logiciels du client.

1.7. Violations et application de la loi

Une violation des directives de sécurité de l'information doit être examinée individuellement et sanctionnée conformément aux dispositions et accords d'entreprise, contractuels et statutaires applicables.

2. Une exigence additionnelle (accès réseau au réseau interne de l'entreprise)

2.1. Définition

Les exigences suivantes doivent être respectées par tous les fournisseurs de services appartenant à l'une des catégories suivantes :

- Les clients (équipements finaux) sont fournis par ALTEN
- La connexion se fait, par exemple, via des solutions VPN avec accès direct au réseau ALTEN et/ou à ceux du client.
- La connexion se fait directement via le réseau ALTEN et/ou celui du client

Ces prestataires de services peuvent tout autant être situés dans leurs propres locaux d'entreprise que sur le terrain d'une installation ALTEN ou du client.

2.2. Exigences

2.2.1. Organisation interne

En ce qui concerne l'utilisation du matériel et des logiciels fournis, les règles et les accords de travail de l'entreprise concernée s'appliquent.

L'ouverture de l'équipement informatique et la modification du matériel (par exemple, l'installation/ le retrait de disques durs, de modules de mémoire) et la modification manuelle des paramètres de sécurité (par exemple, les paramètres du navigateur) ne sont autorisées que par le service concerné (voir l'annexe A.1.4).

L'utilisation ou la modification ultérieure des programmes du Client n'est autorisée que si elle a été approuvée par le service concerné (voir Annexe, A.1. 4).

Les données d'autres clients ne doivent pas être traitées à l'aide de l'équipement informatique fourni.

L'utilisation de logiciels ou de données clients sur des équipements informatiques ou de stockage qui n'ont pas été fournis par le Client ou qui ne sont pas la propriété du Client n'est pas autorisée.

L'utilisation de l'équipement informatique ou des données du client par les employés du fournisseur de services nécessite l'autorisation expresse du client. Le Client est en droit à tout moment d'interdire l'accès ou l'utilisation (par exemple en cas d'utilisation abusive).

2.2.2. Sécurité physique et environnementale

L'équipement fourni doit être manipulé de manière appropriée et doit être protégé contre toute perte ou modification non autorisée.

L'équipement fourni par le Client (par exemple, ordinateurs portables, téléphones portables) ne peut être emporté qu'avec l'autorisation préalable du Client.

2.2.3. Protection contre les logiciels malveillants

Si une attaque par malware est suspectée, les équipements informatiques et supports de données concernés ne doivent plus être utilisés. Le service compétent (voir l'annexe A.1.4) doit être avisé sans délai.

2.2.4. Sauvegarde

Les données doivent être stockées dans les lecteurs réseau alloués et non sur un disque dur local, la raison étant qu'une sauvegarde centrale et automatisée des données n'est garantie que sur le réseau.

L'utilisateur est responsable de la sauvegarde des données qui ne sont pas stockées sur des disques centraux (par exemple, disque dur local, supports de données mobiles).

Les données de sauvegarde et les supports de sauvegarde doivent être traités comme les données d'origine.

2.2.5. Contrôle d'accès

2.2.5.1 Responsabilité de l'utilisateur

Les instructions suivantes doivent être suivies par tous les utilisateurs :

- L'utilisation de l'identifiant d'utilisateur ou du compte d'une autre personne n'est pas autorisée.
- La transmission de moyens d'identification (par exemple, cartes à puce, jetons RSA) n'est pas autorisée.
- Le mot de passe ou le code PIN d'un identifiant d'utilisateur destiné à un usage personnel (appelé « identifiant personnel ») doit être gardé secret et ne doit pas être transmis à une autre personne.
- Dès qu'il y a un soupçon qu'un mot de passe ou un code PIN a été compromis ou est connu , ils doivent être modifiés sans délai.
- Les mots de passe temporaires (par exemple pour les nouveaux comptes) doivent être modifiés lors de la première connexion.
- Tous les mots de passe ou codes PIN doivent être modifiés la première fois qu'ils sont utilisés et au plus tard après 90 jours.
- Il est interdit d'espionner les mots de passe.
- Les mots de passe doivent être classés au moins comme confidentiels.

Si les mots de passe doivent être stockés par écrit, ils doivent être stockés par la personne responsable dans une enveloppe scellée et dans un endroit approprié protégé contre tout accès non autorisé (par exemple dans un coffre-fort).

Chaque fois qu'il est modifié, le mot de passe stocké doit être mis à jour en conséquence. L'enveloppe scellé doit être signé par l'employé concerné.

Les personnes qui ont le droit d'ouvrir l'enveloppe doivent être indiquées par leur nom, car il peut s'avérer nécessaire d'utiliser le mot de passe stocké dans des circonstances exceptionnelles (par exemple, maladie). Ce faisant, la « règle des deux personnes » doit être suivie.

Chaque fois que l'enveloppe est ouverte, elle doit être enregistrée et la personne responsable doit en être informée. Après chaque ouverture, la personne responsable doit changer le mot de passe sans délai et le stocker à nouveau en toute sécurité.

Comme alternative, des systèmes informatiques sont mis en place qui garantissent une fonctionnalité similaire (par exemple, des coffres-forts électroniques par mot de passe).

Lorsqu'il quitte un système pendant le fonctionnement (par exemple, pause, réunion), l'utilisateur doit activer un verrou système (par exemple, un économiseur d'écran protégé par mot de passe).

2.2.5.2 Génération de mots de passe

Lors de la génération d'un mot de passe, les exigences minimales suivantes doivent être remplies :

- Le mot de passe doit comporter au moins 10 caractères, dont au moins trois des 4 types de caractères suivants :
  - Lettres majuscules
  - Lettres minuscules
  - Chiffres
  - Caractères spéciaux
- Si certains systèmes ou applications nécessitent des mots de passe plus complexes, ces spécifications doivent être respectées.
- En particulier, les mots de passe triviaux ne sont pas autorisés (par exemple, « Test1234 ») ou les mots de passe qui incluent une référence personnelle (par exemple, nom, date de naissance).
- Les employés (de l'entrepreneur) ne sont pas autorisés, lorsqu'ils accèdent aux systèmes du client, à utiliser un mot de passe identique à des fins professionnelles et personnelles.
- Les employés (de l'entrepreneur) ne sont pas autorisés à utiliser un mot de passe identique à la fois pour les systèmes qui ont été fournis par ALTEN et les systèmes qui ont été fournis par des tiers (par exemple, les applications, les services d'enregistrement sur Internet).

2.2.6. Contrôle d'accès pour les réseaux

2.2.6.1 Règles d'utilisation des services réseau

Le matériel informatique fourni par le Client ne doit être connecté à un réseau externe (par exemple hotspots, WLAN privé) que si et aussi longtemps que cela est nécessaire pour créer une connexion avec le réseau de l'entreprise (via un accès à distance/VPN).

Une fois que la connexion n'est pas nécessaire, elle doit être déconnectée.

2.2.6.2 Identification des équipements dans les réseaux

Les connexions illimitées d'équipements de communication (par exemple sans pare-feu) au réseau interne (intranet) ne sont autorisées que si elles sont fournies par le Client.

3. Exigences supplémentaires (sans accès direct au réseau interne de l'entreprise)

3.1. Définition

Les exigences énoncées au chapitre 3 doivent être respectées par tous les fournisseurs de services appartenant à l'une des catégories suivantes :

- Prestataires de services n'ayant pas d'accès direct au réseau d'une société du groupe
- Les fournisseurs de services qui ne sont pas fournis avec des terminaux appartenant à une société ALTEN et qui n'utilisent que des appareils finaux appartenant à la société du fournisseur de services.
- Fournisseurs de services qui ne sont pas connectés via un accès à distance ou une autre solution VPN.

Les prestataires de services sont situés dans leurs propres locaux et sont soumis aux règles et règlements de leur propre entreprise.

3.2. Exigences

3.2.1. Organisation interne

Les données des sociétés du groupe doivent être séparées des données de tiers et en particulier des données d'autres clients du prestataire de services (par exemple au moyen de la gestion des droits). Les données ne doivent pas être accessibles par des tiers (par exemple, pour être mises en œuvre au moyen d'un cryptage)

La classification des informations ALTEN doit être incluse dans le diagramme de classification du fournisseur de services afin de s'assurer que toutes les mesures de sécurité nécessaires sont mises en œuvre.

Les prestataires de services doivent afficher les exigences de sécurité des informations tirées des règles et règlements qui leur sont confiés afin d'exécuter la tâche, au moyen de mesures de sécurité appropriées dans leur propre entreprise.

L'accès aux données des clients ne peut être accordé aux employés du fournisseur de services que sur la base du besoin d'en connaître.

4. Obligation de se conformer

Cette règle doit être respectée par tous les fournisseurs de services conformément à la définition du présent document.

Annexe A

Les caractéristiques spécifiques énoncées dans le présent chapitre s'appliquent à une entreprise.

A.1.1 Chaque entrepreneur est responsable de s'assurer que l'information, les programmes et l'équipement de TI ne sont utilisés et utilisés qu'à des fins d'entreprise et dans le cadre de la tâche pertinente.

La transmission de données lorsque le contenu n'est pas lié au travail n'est pas autorisée.

L'utilisation d'Internet à des fins privées n'est autorisée que dans le cadre des règles et réglementations existantes dans l'entreprise.

L'utilisation de logiciels privés et de données sur les équipements informatiques fournis par l'entreprise est interdite.

A.1.2 Les règles suivantes s'appliquent à la sécurité des données et à la protection des données personnelles :

- En termes de classification, les données personnelles qui vont au-delà des données de communication d'entreprise sont considérées comme au moins confidentielles et nécessitent un cryptage technique et une authentification forte (par exemple, un certificat PKI). Tout écart doit être convenu avec le service de protection des données d'ALTEN.
- L'effacement et/ou l'élimination des données des employés est traitée conformément au point A 1.3 ci-dessous, conformément à sa classification.

A.1.3 Les règles suivantes s'appliquent à l'effacement ou à l'élimination des données :

- Les documents papier strictement confidentiels doivent être éliminés à l'aide d'un broyeur de niveau de sécurité P-5 ou supérieur.
- Les documents papier confidentiels doivent être déchiquetés conformément au niveau de sécurité P-4 ou supérieur (bacs de données ou broyeur).
- Avant d'être réutilisés ou éliminés, les supports de données doivent être effacés en effaçant complétement les informations (par exemple, un formatage irréversible) ou en les éliminant de manière appropriée (par exemple, une destruction mécanique).
- Dans la mesure du possible, les supports de données devraient être effacés conformément à la procédure d'effacement des données BSI 2011 ou au moins à la norme 5220.22-M du ministère de la Défense.
- Si le support de données est un disque dur SSD ou généralement un lecteur flash, il est obligatoire d'utiliser la méthode Gutmann.
- Les supports de données qui ne sont plus nécessaires doivent être effacés de manière fiable en les écrasant ou en les détruisant physiquement.
- La destruction des disques durs et autres supports de stockage doit être enregistrée et doit être effectuée par une entreprise d'élimination certifiée.
- Les supports de données optiques (CD, DVD, Blu-ray, etc.) etles bandes magnétiques doivent également être physiquement détruits afin d'assurer l'effacement fiable des informations stockées.

A.1.4 Information Security Team: ODCInformationsecurity@alten.com

A.1.5 Coordinateur protection des données personnelles : privacy-maroc@alten.com