Directive relative à la sécurité des informations.

amag

Table des matières

1. Introduction

La présente directive s'applique à l'ensemble du groupe AMAG et à ses collaborateurs, ainsi qu'aux parties tierces qui détiennent ou traitent les informations du groupe AMAG, ou qui collectent des informations sur mandat du groupe AMAG. Les parties tierces doivent être liées par contrat à la présente directive ou fournir une indication claire et vérifiable précisant qu'elles sont elles-mêmes soumises à une directive comparable et qu'elles la respectent. L'expression «Collaborateurs» sera utilisée dans ce qui suit à la fois pour les employés du groupe AMAG et pour les collaborateurs de parties tierces.

Les mesures de sécurité décrites protègent les collaborateurs du groupe AMAG (et des parties tierces au sens évoqué précédemment) ainsi que les clients du groupe AMAG et les visiteurs. En outre, ces exigences contribuent à protéger les biens matériels et immatériels du groupe AMAG et à répondre aux dispositions légales.

2. Principes de base

L'énumération suivante présente un aperçu des principes de base de la sécurité des informations au sein du groupe AMAG et fait office de récapitulatif.

1. La sécurité des informations est l'affaire de tous les collaborateurs du groupe AMAG dans le cadre de leur mission et de leur travail. Les collaborateurs prennent leur responsabilité en respectant la présente directive.
2. En matière de traitement et de transfert de données, il doit être garanti que seules les personnes autorisées aient accès à ces données. Il convient de faire preuve de retenue dans l'attribution de droits (de lecture comme d'écriture): c'est le principe du «need-to-know» et du «need-to-do». Plus les données sont largement divulguées, plus la probabilité de voir des données confidentielles apparaître à des endroits inopportuns augmente.
3. Lors de l'utilisation d'outils informatiques, les données sauvegardées, traitées ou exploitées autrement doivent être traitées en fonction de leur besoin de confidentialité. Il convient en particulier d'éviter que des données confidentielles ou liées aux personnes ne tombent entre les mains de personnes non autorisées.
4. Les supports de données inconnus tels que par exemple les clés USB trouvées ne doivent pas être utilisés. Les supports de données inconnus trouvés dans les locaux ou dans les enceintes du groupe AMAG doivent être remis au personnel informatique en indiquant le lieu et l'heure de leur découverte.
5. La vigilance est de rigueur dans l'utilisation d'Internet, en particulier concernant les services inconnus ou apparemment douteux. La protection contre les logiciels truqueurs et la prévention des préjudices de réputation revêtent une priorité absolue.
6. Pour exclure le plus possible les logiciels malveillants, il est recommandé de filtrer les transferts sur Internet du groupe AMAG (web, e-mail, chat, etc.) afin que ces transferts bloquent les contenus indésirables, voire dangereux. Ces filtres fonctionnent conformément aux dispositions de la législation suisse en matière de protection des données. Aucune évaluation régulière du comportement d'utilisation des collaborateurs n'est réalisée.

7. Les pièces jointes d’e-mails ne doivent être ouvertes que par des expéditeurs connus. En cas de doute, il faut avertir le service de sécurité informatique.
8. Les mots de passe sont individuels, personnels et ne doivent pas être transmis.
9. Les clés de porte, cartes d’accès (KABA), etc. personnelles ne doivent être transmises à quiconque, ni même à des membres de l’équipe.
10. Les clés ou cartes d’accès (KABA) non personnelles telles que par exemple les clés générales d’accès aux entrepôts, ne doivent être transmises qu’à des personnes autorisées. En cas de doute, il convient de définir auprès du supérieur hiérarchique les personnes habilitées à les utiliser. L’utilisation de clés ou de cartes d’accès non personnelles doit être consignée (qui, quand, combien de temps, quelle clé).
11. Aucune donnée d’affaires ne doit être transmise à des personnes inconnues ou non autorisées. Cela vaut aussi bien pour la communication orale que pour la remise ou la transmission de données par e-mail, clés USB, autres supports de données électroniques, imprimés ou par des moyens similaires.
12. En cas de doute quant à l’autorisation, il convient de clarifier auprès de son supérieur hiérarchique si la personne est habilitée à consulter ou à obtenir les données en question.
13. Il ne faut pas permettre à des personnes inconnues d’accéder à des zones qui ne sont pas accessibles au public. Cela concerne les zones non publiques situées dans les bâtiments, les enceintes barricadées, les entrepôts, etc.
14. Les visiteurs externes à l’entreprise doivent être annoncés au préalable et inscrits sur une liste des visiteurs lorsqu’ils sont guidés dans des zones non publiques.
15. Il faut s’abstenir de parler d’informations confidentielles dans les espaces publics. Cela concerne notamment mais pas uniquement les transports publics, les restaurants, etc. En particulier lors des repas d’affaires, il faut veiller que les tables voisines ne puissent pas entendre d’informations confidentielles.

3. Mots de passe, clés, etc.

Les mots de passe, clés, etc. permettent d’accéder à des systèmes, à des données et donc à des informations. La bonne gestion des mots de passe, des clés de portes, portails, coffres-forts, etc. revêt donc une grande importance pour tous les objectifs de sécurité.

3.1 Mots de passe

Les mots de passe personnels ne doivent pas être transmis, que ce soit à des membres de l’équipe, à des collaborateurs du service informatique internes ou externes, ou à d’autres cercles de personnes. S’il y a suspicion qu’un mot de passe a été deviné, il doit être modifié immédiatement.

Lors du choix d’un mot de passe, veiller à respecter les exigences de mot de passe enregistrées dans les systèmes. Dans la mesure du possible, il est recommandé d’opter pour un mot de passe long, une «phrase de passe» ainsi nommée (phrase de passe plutôt que mot de passe).

Une phrase de passe peut par exemple contenir une combinaison d'abréviations, de mots complets et de chiffres, plutôt que de n'utiliser que des lettres. Si quelqu'un aime la photographie, il pourrait alors opter pour la phrase complète suivante: «La photographie est mon plus grand hobby!» et deux des multiples traductions possibles pourraient être «PhestmonplugrandH0661!» ou «Foto4everpourmoi». Ces deux phrases de passe ne doivent naturellement pas être utilisées.

3.2 Cartes d'accès (badges)

Dans les environnements dans lesquels des cartes d'accès personnelles (badges) sont utilisées, celles-ci ne doivent pas être transmises à d'autres collaborateurs, à des collaborateurs de parties tierces ou à des visiteurs.

L'utilisation de cartes d'accès non personnelles doit être consignée (qui, quand, combien de temps, quelle carte).

3.3 Clés physiques

On entend dans le présent document par clés physiques les clés conventionnelles que l'on utilise habituellement pour les portes de bâtiments ou de pièces, parfois également pour les coffres-forts.

Les clés physiques personnelles ne doivent pas être transmises. Elles doivent être conservées en permanence à un endroit sécurisé, par exemple en portant la clé «sur la personne».

Les clés utilisées par plusieurs personnes, par exemple par une équipe, doivent être conservées durant la nuit soit dans un coffre-fort sécurisé par une combinaison de chiffres, soit être emportées par le responsable.

L'utilisation de clés physiques non personnelles doit être consignée (qui, quand, combien de temps, quelle clé).

4. Utilisation d'outils informatiques

Les ordinateurs mis à la disposition du personnel par le groupe AMAG (ordinateur portable, téléphone mobile, etc.) ainsi que les programmes et les données sont destinés à un usage professionnel et doivent être utilisés avec précaution (éviter les vols, les détériorations, l'accès de tiers aux appareils, etc.). Les appareils laissés sans surveillance doivent être bloqués. L'utilisation d'ordinateurs privés (par exemple de téléphones mobiles privés) et de logiciels qui n'ont pas été fournis par le groupe AMAG est possible mais dans ce cas également, les mesures de précaution citées s'appliquent.

La même attention est requise de manière générale lors de l'utilisation d'Internet et de ses services; voir également à cet effet le chapitre «Internet, réseaux sociaux, chat, e-mail».

Concernant la protection contre l'ingénierie sociale (manipulation sociale), il faut veiller que les informations confidentielles ne soient pas transmises par le biais du téléphone, d'entretiens directs ou d'autres canaux (e-mail, chat, etc.) à des personnes qui ne sont pas clairement identifiées.

Les données qui ne sont plus requises, à savoir les données qui n'ont plus d'objectif économique et qui

ne sont soumises à aucune obligation légale de conservation (par exemple les e-mails purement internes), devraient être effacées ou supprimées. Cette clause s'applique également aux données sur papier.

5. Internet, réseaux sociaux, chat, e-mail

Internet doit être utilisé en premier lieu à des fins commerciales. Il peut être utilisé raisonnablement à des fins privées. Cela signifie que les e-mails, les autres services de communication et les réseaux sociaux, les forums de chat, les blogs, etc. sont permis dans le cadre d'une utilisation personnelle. L'utilisation de moyens de communication à des fins privées ne doit pas nuire à l'activité de travail des collaborateurs. Il faut veiller en permanence que les informations puissent être difficilement supprimées d'Internet ou qu'elles ne le puissent pas du tout.

La communication publique en revanche est l'affaire du service de communication. Il est le seul à pouvoir publier pour le groupe AMAG sur des canaux visibles par le public: sites web, Twitter, Facebook, etc. au nom du groupe AMAG. Les besoins de communication éventuels doivent faire l'objet d'une concertation auprès de la Group Communication.

Malgré les nombreux avantages que procure Internet, tous les types de logiciels malveillants tels que les virus, chevaux de Troie, courriels d'hameçonnage, etc. sont malheureusement répandus via Internet. En règle générale, les logiciels malveillants sont distribués par le biais de sites web infectés ou d'e-mails. AMAG filtre les e-mails entrants à la recherche de maliciels. Il se peut toutefois que des e-mails individuels qui contiennent des logiciels malveillants dissimulés en particulier dans les pièces jointes, soient envoyés. Il faut traiter avec la plus grande précaution les e-mails d'expéditeurs inconnus ou ceux présentant des formulations «atypiques». Malgré les programmes de protection existants tels que les logiciels antivirus, l'ouverture d'e-mails ou de pièces jointes comprenant des maliciels peut conduire à de graves dommages. Si un doute existe quant à la présence d'un programme malveillant, il convient de faire immédiatement part de ce doute à l'adresse it-systems.network@amag.ch

6. Sécurité physique

Ce chapitre décrit les principes de la protection physique. L'objectif principal est la protection de toutes les personnes qui se trouvent sur les terrains et dans les bâtiments du groupe AMAG, ainsi que la protection de tous les biens immobiliers, outils, machines, stocks, équipements de bureau, matériaux informatiques et autres effets de valeur du groupe AMAG.

6.1 Principes directeurs

L'accès à l'enceinte, aux bâtiments et aux espaces situés à l'intérieur de bâtiments non accessibles au public doit être accordé uniquement aux personnes autorisées qui requièrent un accès dans le cadre de leur travail (principe du «Need-to-know» et surtout du «Need-to-do»).

6.2 Portails et portes

Les portes et les passages qui séparent les différents espaces tels que les bureaux, halles de garage ou entrepôts, peuvent être équipés de systèmes de sécurité supplémentaires. Ces mécanismes de protection ne doivent pas être désactivés. Par exemple, les clés ou cartes d'accès ne doivent pas être transmises à

des personnes non autorisées, en particulier à des visiteurs. Les clés ou cartes d'accès personnelles ne doivent être transmises en aucun cas.

6.3 Responsabilités

La responsabilité de la sécurité physique incombe au responsable de la sécurité compétent pour le site. Le responsable de la sécurité doit garantir que des mesures de sécurité suffisantes soient adaptées pour la mise en œuvre de la présente directive et soient conformes aux exigences concrètes des environnements concernés. Dans ce but, le responsable de la sécurité organise des contrôles (audits) en cas de besoin.

Il incombe au responsable de la sécurité de garantir que les mesures de sécurité physique nécessaires ont été prises. En cas de besoin, le responsable de la sécurité doit se faire conseiller dans ce domaine.

7. Visiteurs

Au sens de la présente directive, sont considérées comme des visiteurs toutes les personnes qui ne font pas partie du personnel du groupe AMAG et qui ne disposent pas d'un poste de travail permanent au sein du groupe AMAG. Les énumérations suivantes sont valables pour les zones non publiques. Les showrooms ou les cantines accessibles au public par exemple ne font pas partie de cette énumération.

Les visiteurs doivent être annoncés au préalable par un collaborateur ayant un poste de travail permanent au sein du groupe AMAG, et être enregistrés avec leur nom, le nom de la société, la date et le motif de la visite dans la liste des visiteurs du site concerné. La personne qui se présente comme hôte pour la visite est responsable du visiteur.

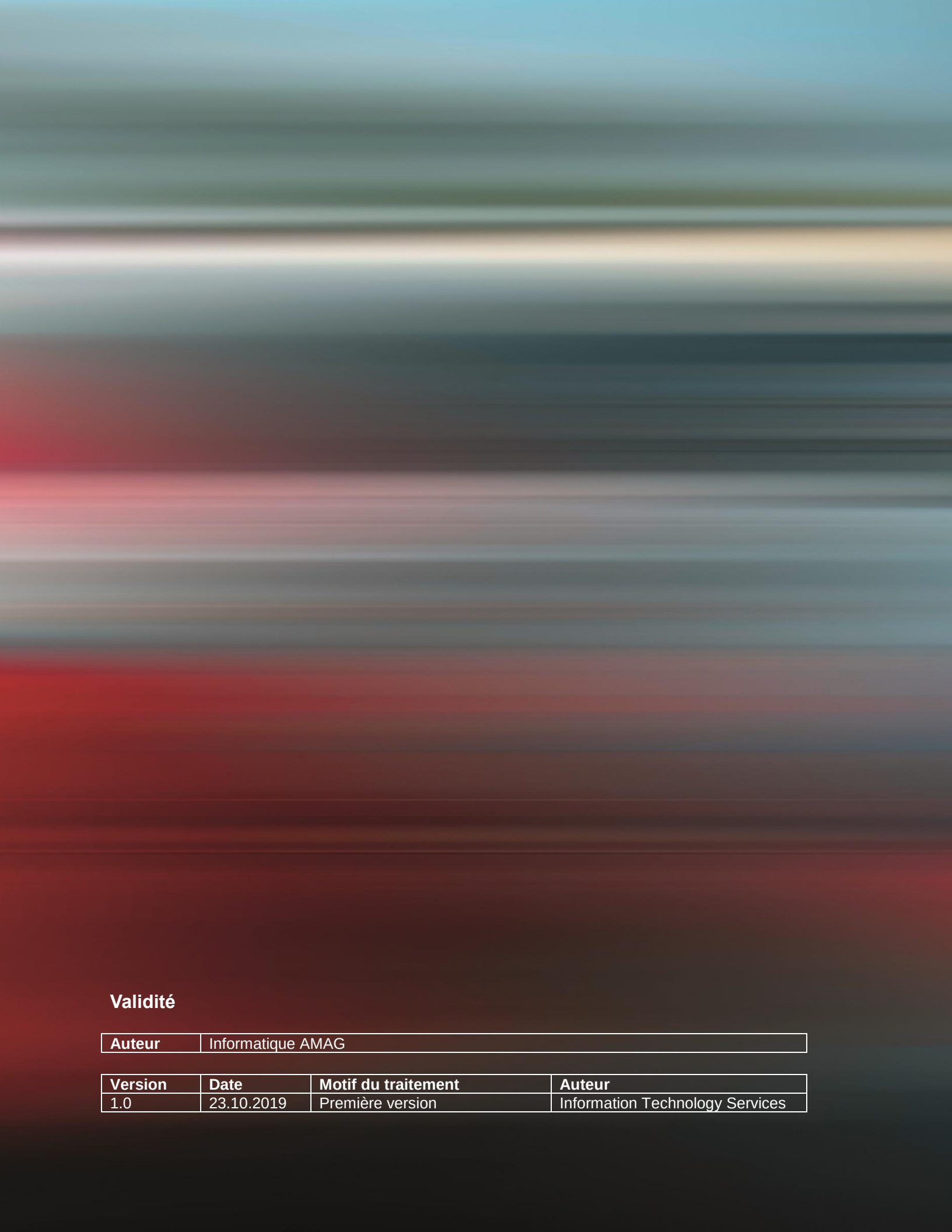
8. Surveillance

L'objectif de la surveillance est la protection des données et de l'infrastructure informatique. Des filtres peuvent être utilisés contre les maliciels, contre les sites web qui répandent des logiciels malveillants ou dangereux, ou contre les serveurs dont l'utilisation pourrait représenter un problème pour la réputation. De plus, la surveillance doit détecter les attaques à l'encontre de l'environnement du groupe AMAG à partir d'Internet et d'Intranet.

Aucune surveillance régulière des personnes n'est réalisée. Le groupe AMAG respecte la législation suisse en matière de protection des données.

9. Annexe – Restriction de l'information et des données

Impression	**Définition dans le cadre de la présente directive**	**Exemples**
Données	Information sur un support de sauvegarde ou de transfert	Impressions sur papier / fichiers informatiques / e-mails / sites web / etc.
Information	Le véritable message / contenu	Message / déclaration / instruction / description



Validité

Auteur	Informatique AMAG

Version	Date	Motif du traitement	Auteur
1.0	23.10.2019	Première version	Information Technology Services