Revision : 01.06.2024 **QM : A. Christen** **Validation : F. Studer & S. Weiss** **P1-05-F19-fr**

Règlement d'utilisation IT

Sommaire

1. Définitions des termes 2
2. Objectif et champ d'application 3
3. Champ d'application personnel 3
4. Conséquences 3
5. Organisation et responsabilités 3
6. Obligations des collaborateurs 4
7. Règles générales d'utilisation de l'infrastructure IT 4
7.1 Respect du cadre juridique 4
7.2 Traitement des données 4
7.3 Acquisition, utilisation et maintenance de logiciels 4
8. Protection minimale de la sécurité informatique 5
8.1 Règlement d'entrée et d'accès aux locaux et aux données 5
8.2 Mots de passe 5
8.3 Pare-feu et protection antivirus 5
9. Stockage des données 5
9.1 Principe 5
9.2 Sauvegarde des données, backup & restore et archivage 6
9.3 Accès à distance au réseau interne 6
9.4 Traitement des données après le départ d'un collaborateur 6
9.5 Déviation des e-mails entrants en cas d'absence soudaine / de départ 6
10. Règles spécifiques à la communication 7
10.1 Généralités 7
10.2 Transfert d'e-mails 7
10.3 Gestion de la boîte aux lettres électronique et suppléance 7
11. Confidentialité / suivi 7
11.1 Intérêts de Galliker 7
11.2 Faire valoir ses droits vis-à-vis de tiers et des collaborateurs 7
11.3 Intérêts de nos colaborateurs 7
11.4 Mesures concrètes de consignation et de suivi 8
11.5 Contrôle / évaluation 8
11.5.1 Accès aux protocoles 8
11.5.2 Accès aux e-mails et aux documents relevants 9
11.5.3 Utilisation à des fins privées 9
11.6 Déclaration de consentement 9
12. Sécurité des appareils mobiles 9
12.1 Responsabilité 9
12.2 Travaux d'entretien ou de réparation et élimination par des organismes agréés 10
12.3 Précautions à prendre avant les travaux d'entretien ou de réparation, le remplacement et l'élimination 10
13. Assistance générale aux utilisateurs 10
14. Réseau et accès à Internet 10
15. Formation des collaborateurs 10
16. Entrée en vigueur 10

1. Définitions des termes

Terme	Définition
Traitement	Toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, la conservation, l'utilisation, la transformation, la communication, l'archivage ou la destruction de données (cf. art. 5 lit. d nLPD). Correspond à la notion de « traitement » selon l'ar. 4 chiff. 2 RGPD : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
Données	Informations de toute nature, notamment les données physiques telles que les documents papier, les contrats, les carnets de notes, les lettres et les factures, ou encore les données électroniques telles que les courriers électroniques, les documents électroniques et les enregistrements audio et vidéo. Les données personnelles en font également partie.
Propriétaire des données	Personne ou poste au sein de Galliker qui est responsable de certaines données et qui, avec le conseiller de la protection des données, garantit le respect des règles et des directives en matière de traitement des données.
Conseiller à la protection des données	Galliker a nommé un conseiller à la protection des données, joignable à l'adresse dsb@galliker.com. Celui-ci est l'interlocuteur pour les personnes concernées et pour les autorités chargées de la protection des données en Suisse. Le conseiller à la protection des données forme et conseille Galliker sur les questions de protection des données et concourt à l'application des prescriptions relatives à la protection des données (art. 10 nLPD). Dans l'UE, le conseiller à la protection des données fait office de délégué à la protection des données conformément à l'art. 37 RGPD.
Services	Tous les services qui sont nécessaires à l'accomplissement de l'objectif du groupe Galliker. Les services à usage personnel n'en font pas partie.
Galliker	Toutes les entreprises du groupe Galliker selon l'organigramme actuel.
Supports d'information	Tous les supports, notamment le papier et les autres supports de données (électroniques), sur lesquels des données peuvent être consignées..
Infrastructure IT	Moyens électroniques de communication, d'information et autres moyens techniques, en particulier tous les appareils ou composants qui peuvent être utilisés pour le traitement, le stockage ou le transport de données, tels que PC, ordinateur portable, téléphone mobile, PDA, smartphone & smartwatch, clé USB, CD, DVD ou autres supports de sauvegarde ou services et le réseau.
Classification des données	Indique le besoin de protection des données. La classification donne des informations sur le type d'accès, les autorisations d'accès et de modification, la transmission des données, la sauvegarde des données et les règles d'archivage, les règles de traitement des impressions sur papier/tableau blanc et les règles d'effacement.
Appareils mobiles	Téléphones mobiles, smartphones (téléphones mobiles dotés de fonctions avancées de saisie, de stockage, de transmission et d'affichage de données de toute sorte), y compris les appareils privés.

Données personnelles	Toutes les informations concernant une personne physique identifiée ou identifiable (cf. art. 5 let. a nLPD). Correspond à la notion de « données à caractère personnel » selon l'art. 4 chiff. 1 RGPD : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
Appareils privés	Appareils mobiles achetés par un participant avec ses propres moyens (sans remboursement par Galliker).

2. Objectif et champ d'application

Le présent règlement d'utilisation IT régit l'utilisation des moyens électroniques de communication, d'information et autres moyens techniques (ci-après infrastructure IT) et des données de Galliker. Le règlement d'utilisation IT est dérivé de la stratégie de sécurité informatique et en déduit des exigences organisationnelles et techniques concrètes qui s'appliquent à tous les projets et processus, indépendamment des services spécifiques. Il est complété par des directives spécifiques selon le processus ISO P3-09. Galliker peut à tout moment adopter d'autres directives.

Le présent règlement d'utilisation IT doit être obligatoirement respecté par les collaborateurs lorsqu'ils utilisent l'infrastructure informatique à des fins professionnelles.

3. Champ d'application personnel

Ce règlement d'utilisation IT est obligatoire pour les collaborateurs ou pour toutes les personnes ayant **accès aux données et/ou à l'infrastructure IT de Galliker**, qu'il s'agisse d'entrepreneurs, d'étudiants, de stagiaires, d'intérimaires, de fournisseurs, de sous-sous-traitants, de professions libérales ou d'autres partenaires (ci-après uniquement les collaborateurs).

4. Conséquences

Les infractions au règlement d'utilisation IT peuvent entraîner des mesures relevant du droit du travail et des conséquences civiles et pénales. Ainsi, un avertissement peut être adressé, l'accès à Internet peut être bloqué, des dommages et intérêts peuvent être réclamés, les bonus et les primes spéciales peuvent être supprimés. Dans les cas extrêmes, comme par exemple en cas d'abus répétés avec dysfonctionnement technique malgré un avertissement ou en cas de délit avéré, Galliker peut prononcer le licenciement, faire valoir des prétentions civiles et/ou déposer une plainte pénale.

Les supérieurs hiérarchiques ainis que l'administration du système sont responsables du contrôle du respect de ces règles.

5. Organisation et responsabilités

L'organisation et les responsabilités informatiques sont régies par le GIPF (Galliker IT Process Framework).

6. Obligations des collaborateurs

Les collaborateurs doivent respecter les obligations générales suivantes :

- Devoir de diligence : utilisation soigneuse et légale de l'infrastructure IT, des données et des ressources qui y sont liées, en particulier aussi des appareils privés, en évitant notamment de diffuser des contenus comme suit :
    - représentations de la violence au sens de l'art. 135 du Code pénal suisse (CP)
    - écrits, images et représentations pornographiques au sens de l'art. 197 al. 1 et 3 CP
    - discrimination raciale au sens de l'art. 261bis CP
    - incitations à la violence au sens de l'art. 259 CP
    - instruction ou incitation à des comportements délictueux ou leur encouragement d'une autre manière
    - jeux de hasard non autorisés
    - autres contenus illicites,
- Respecter les principes de base de la protection des données, quelle que soit la technologie choisie, conformément à la ⇨ **directive sur la protection des données**,
- Obligations de notification : Signaler immédiatement tout incident, tel qu'un comportement étrange de l'infrastructure informatique, la perte ou l'abus présumé de données et/ou de l'infrastructure IT,
- Sécurité : respect strict de toutes les consignes et directives de sécurité,
- Comportement : l'infrastructure IT ne doit être utilisée que dans le cadre de l'éthique, de la morale et de la légalité.

7. Règles générales d'utilisation de l'infrastructure IT

7.1 Respect du cadre juridique

Lors de l'utilisation de l'infrastructure IT, les lois, réglementations et directives (internes) pertinentes doivent être respectées. Il s'agit par exemple de la protection des données, des obligations de conservation et d'effacement, des lois sur les droits d'auteur, des règles de protection contre les incendies, de toutes les directives des collaborateurs ou les contrats avec les clients.

7.2 Traitement des données

Des propriétaires sont définis pour les processus commerciaux, les données, les services et les systèmes IT (⇨ **directive organisation IT et responsabilités**).

Toutes les données doivent être classées en fonction de leur besoin de protection (⇨ concept de classification).

L'objectif est de traiter les données en fonction de leur besoin de protection. Ce n'est que lorsque les collaborateurs et surtout les propriétaires des données savent quelles informations nécessitent une protection particulière qu'ils peuvent les protéger de manière adéquate. Du besoin de protection des données découle en fin de compte le besoin de protection des systèmes IT sur lesquels les données sont traitées.

Les propriétaires des données définissent qui ou quels rôles peuvent accéder aux données ou utiliser les services et les systèmes IT, et sous quelles conditions.

Lors du traitement de données personnelles, les collaborateurs respectent la protection des données et veillent à la confidentialité, à la disponibilité, à l'intégrité et à la pérennité des données.

Tant les services informatiques que les supérieurs hiérarchiques de Galliker doivent protéger les données personnelles qu'ils traitent dans le cadre d'une surveillance par des mesures techniques appropriées contre tout accès non autorisé.

7.3 Acquisition, utilisation et maintenance de logiciels

Les collaborateurs ne peuvent pas se procurer (ni télécharger), utiliser ou entretenir de nouveaux services (surtout des logiciels) et les installer sur leur infrastructure IT professionnelle sans l'autorisation des services IT. Cette règle ne s'applique pas aux logiciels destinés aux appareils personnels.

8. Protection minimale de la sécurité informatique

8.1 Règlement d'entrée et d'accès aux locaux et aux données

Les collaborateurs ne doivent pas accorder l'accès aux locaux et aux données de Galliker à des personnes non autorisées sans que l'accès soit enregistré. Les invités ne doivent pas se déplacer librement et sans contrôle dans les locaux de Galliker. Un contrôle des clés ou un contrôle par badge doit être effectué. Si des préposés, des agents ou d'autres tiers mandatés ont accès aux données de Galliker, l'accès et toutes les actions sont consignés.

Chaque collaborateur ainsi que les préposés, agents ou autres tiers mandatés disposent d'autorisations individuelles pour accéder aux locaux, aux services et à l'informatique ainsi que pour accéder aux données. Le propriétaire des données accorde les autorisations correspondantes.

L'authentification des droits d'accès est assurée par un nom d'utilisateur et des mots de passe. Les règles suivantes concernant les mots de passe s'appliquent.

En quittant le poste de travail, l'ordinateur doit être verrouillé.

8.2 Mots de passe

Les collaborateurs doivent protéger l'infrastructure IT qu'ils utilisent à des fins professionnelles par un mot de passe sécurisé.

Un mot de passe est sûr lorsqu'il

- se compose d'au moins 10 caractères
- contient au moins des lettres (majuscules et minuscules), des chiffres et des caractères spéciaux
- ne comporte pas de répétitions successives de plus de deux caractères identiques
- n'est pas identique aux anciens mots de passe
- n'est pas une répétition des dix derniers mots de passe
- ne contient pas de faits connus de tous, tels que le nom de l'épouse/du mari, des enfants, des animaux domestiques, la rue, les dates de naissance, les numéros d'immatriculation, les numéros de téléphone, etc.
- n'est pas déjà utilisé sur d'autres plateformes.

Les mots de passe ne doivent pas être notés, en particulier sur ou autour de l'infrastructure IT. Les mots de passe peuvent être gérés dans le gestionnaire de mots de passe. Les mots de passe ne doivent pas être transmis à d'autres personnes. Le service IT peut imposer techniquement le respect des prescriptions en matière de mots de passe. Les cadres et les collaborateurs disposant de fonctions et de droits d'accès étendus doivent respecter des consignes plus strictes en matière de mots de passe, ce qui se répercute avant tout sur la longueur du mot de passe.

8.3 Pare-feu et protection antivirus

La connexion à un réseau externe ne peut se faire qu'après l'introduction d'un pare-feu approprié. Le pare-feu doit être configuré et administré de manière à assurer une protection efficace et à empêcher les manipulations.

Les collaborateurs ne doivent ni désactiver ni supprimer les programmes de protection contre les virus installés par Galliker. Les mises à jour doivent être installées immédiatement après leur validation par les services IT.

Les contenus actifs doivent être filtrés de manière centralisée au niveau du pare-feu. Pour le pare-feu, les règles de filtrage doivent être aussi restrictives que possible (« *tout ce qui n'est pas autorisé est interdit* »). Les collaborateurs ne doivent toutefois pas être importunés par une multitude de messages et être gênés dans leur travail.

Si les collaborateurs constatent des irrégularités dans l'utilisation de leur infrastructure IT, ils doivent en informer immédiatement les services IT.

9. Stockage des données

9.1 Principe

Les données de Galliker doivent toujours être enregistrées sur l'infrastructure centrale et non sur le bureau ou sur un appareil mobile. Tous les e-mails entrants et sortants sont enregistrés de manière automatisée. Il n'est pas possible d'exclure les e-mails privés. Seules les données avec la classification de données publique (voir

⇨ **concept de classification**) peuvent être enregistrées dans le cloud public ou sur le site web de Galliker. En outre, l'utilisation de services en cloud ou le stockage sur des appareils mobiles non autorisés sont interdits.

Le traitement des données ne peut se faire que sur l'infrastructure IT qui a été validée par Galliker. Les données importantes pour l'entreprise, y compris les données des clients, ne doivent donc pas être envoyées ou traitées via des sites web non autorisés, des logiciels non autorisés, des réseaux privés et non sécurisés. La transmission de données à des tiers et à des personnes non autorisées est interdite.

L'envoi et le traitement de données importantes pour l'entreprise ainsi que de données clients ne doivent avoir lieu que dans l'intérêt de l'entreprise et uniquement via des canaux cryptés.

Les services IT sont soumis au secret professionnel et agissent dans l'intérêt de Galliker dans le respect des dispositions légales.

9.2 Sauvegarde des données, backup & restore et archivage

Il n'y a pas de sauvegarde/backup pour les données sur le bureau.

Aucune sauvegarde de données n'est effectuée pour les appareils mobiles. Toutes les informations affichées, stockées, traitées et transmises sur des appareils mobiles doivent être protégées d'une autre manière ou les modèles d'entreprise doivent être conçus de manière à ce qu'il n'y ait aucun dommage en cas de perte des données sur les appareils mobiles.

Une fois une transaction terminée, les données et les e-mails doivent être archivés. La ⇨ **directive d'archivage et de suppression** s'applique.

9.3 Accès à distance au réseau interne

En général, l'accès sur place est préférable à l'accès « à distance ».

Une connexion externe au réseau interne doit être assurée par des mesures appropriées et est prescrite par les services IT.

La technologie de cryptage utilisée devrait, dans la mesure du possible, être basée sur la technologie de l'appareil mobile et, si elle est connue et publiée, faire l'objet d'une évaluation par des experts.

9.4 Traitement des données après le départ d'un collaborateur

Si un collaborateur est absent à court terme pour une longue période ou s'il quitte l'entreprise à la suite d'un licenciement sans préavis, d'une mise à pied ou d'une démission régulière, l'employeur est autorisé à disposer librement des données de messagerie de la personne concernée afin de préserver et de poursuivre les intérêts de l'entreprise, dans le respect des directives de protection des données.

Avant de quitter l'entreprise, le collaborateur doit transmettre en interne les affaires et les e-mails encore en suspens.

Le collaborateur doit confirmer par écrit la remise de tous les documents commerciaux à Galliker.

Le collaborateur qui quitte l'entreprise a la possibilité de sauvegarder ses e-mails privés et autres données sur des supports de données privés et de les effacer des serveurs de l'entreprise.

En cas de départ, Galliker bloque le compte e-mail de la personne concernée (comme d'ailleurs tous les autres comptes informatiques) au plus tard le dernier jour de travail et efface sa boîte aux lettres (comme tous les autres supports de données personnels). Les e-mails du compte e-mail sont sauvegardés conformément à la ⇨ **directive d'archivage et de suppression**.

Les expéditeurs qui envoient des e-mails à l'adresse e-mail bloquée sont automatiquement informés que le collaborateur ne travaille plus pour Galliker. La réponse automatique indiquera une adresse électronique de remplacement appropriée de Galliker.

9.5 Déviation des e-mails entrants en cas d'absence soudaine / de départ

Si un collaborateur est absent pour une longue période en raison d'un cas de force majeure (accident, maladie, décès) ou s'il quitte l'entreprise suite à un licenciement sans préavis, une mise à pied ou un départ régulier, l'employeur est autorisé à disposer librement des données de messagerie de la personne concernée afin de préserver et de poursuivre les intérêts de l'entreprise, dans le respect des directives relatives à la protection

des données et de la politique de conservation et de suppression des données. En cas de décès, le compte de messagerie du défunt est immédiatement bloqué et les données sont sauvegardées.

En outre, en cas de départ, les dispositions du paragraphe 9.4 ci-dessus s'appliquent.

10. Règles spécifiques à la communication

10.1 Généralités

Le traitement, l'accès, le stockage et le niveau de sécurité des données et des informations sont régis par le ⇨ **concept de classification**. Les données et les informations sont traitées et stockées de manière sécurisée.

10.2 Transfert d'e-mails

Lors d'une transmission automatique de courriels, la confidentialité doit être préservée en s'assurant que tous les destinataires sont également autorisés à lire les courriels conformément au concept de classification.

10.3 Gestion de la boîte aux lettres électronique et suppléance

Chaque boîte aux lettres électronique doit être consultée au moins une fois par jour. Si un collaborateur est absent pendant une période prolongée, il doit déposer un message correspondant dans sa boîte aux lettres électronique. Ainsi, pendant son absence, un expéditeur reçoit du destinataire un message automatique indiquant le type et la durée de l'absence ainsi que le nom du remplaçant (personne à contacter avec numéro de téléphone / adresse e-mail).

L'échange de mots de passe entre collaborateurs est interdit. L'utilisation de cette fonction avec un destinataire extérieur à Galliker, c'est-à-dire le transfert automatique vers un compte de messagerie, est à proscrire pour des raisons de sécurité.

11. Confidentialité / suivi

11.1 Intérêts de Galliker

L'utilisation de moyens de communication électroniques peut porter atteinte aux intérêts et aux installations techniques suivants de Galliker :

- capacité de stockage et bande passante du réseau en raison d'une utilisation excessive d'Internet et du courrier électronique,
- sécurité des données et des applications (disponibilité, intégrité, confidentialité) par l'importation de logiciels malveillants (virus, vers, chevaux de Troie, bots, etc.) ou l'installation de programmes étrangers,
- utilisation du temps de travail (perte de productivité) ainsi que d'autres intérêts financiers (augmentation des coûts pour des moyens et/ou des prestations supplémentaires, coûts de réseau, etc.),
- autres intérêts protégés par la loi, tels que les secrets commerciaux, la protection des données ou le maintien de la confidentialité vis-à-vis du client.

11.2 Faire valoir ses droits vis-à-vis de tiers et des collaborateurs

Pour faire valoir des droits et remplir des obligations légales vis-à-vis de tiers et de collaborateurs, Galliker doit pouvoir accéder aux e-mails ou à d'autres documents commerciaux relevants des collaborateurs, en plus des possibilités de contrôle et de surveillance selon paragraphe 11.6. Cela vaut également pour les e-mails archivés ou la documentation commerciale relevante. La procédure d'un tel accès s'effectue conformément au paragraphe 11.6.

11.3 Intérêts de nos colaborateurs

Galliker respecte et protège la personnalité de ses collaborateurs dans le cadre des rapports de travail, prend dûment en considération leur santé et veille à la préservation de la moralité. Galliker utilise des systèmes pour consigner le comportement d'utilisation des collaborateurs en ce qui concerne les moyens de communication électroniques. Les données ainsi obtenues ne sont traitées que si elles sont pertinentes pour l'entreprise ou la sécurité. Il est garanti que ces données sont toujours traitées de manière confidentielle et qu'elles ne sont

accessibles qu'à un nombre très limité de personnes. Avec ces mesures, Galliker ne surveille pas systématiquement le comportement des collaborateurs sur le lieu de travail, ce qui est interdit par la législation locale du travail (par ex. pour la Suisse, art. 26 OLT 3).

11.4 Mesures concrètes de consignation et de suivi

L'infrastructure IT effectue des enregistrements sur les principales activités réalisées, c'est-à-dire que les données marginales « qui », « quoi » et « quand » sont enregistrées en permanence. Chez Galliker, la journalisation a lieu aux endroits suivants :

- e-mail à des fins d'archivage et de preuve pour la durée de l'obligation légale de conservation des données pertinentes pour l'entreprise, en particulier des prétentions juridiques de tiers (dans le cadre de mesures civiles, pénales et administratives),
- trafic d'e-mails, pour la mise en œuvre de directives techniques visant à protéger l'entreprise, et pour la surveillance des attaques ou des pertes de données,
- utilisation d'Internet à des fins de preuve et de respect des prescriptions légales pour une durée de 6 mois ; les enregistrements par caméra sont effectués pour une durée de 14 jours. Le but et le contenu des enregistrements sont l'accès à la protection du périmètre ; le ⇨ **règlement vidéo** contient de plus amples informations
- événements système sur les postes de travail contenant des processus et des services exécutés, avec une durée de conservation de 30 jours.

11.5 Contrôle / évaluation

11.5.1 Accès aux protocoles

Pour contrôler le respect du règlement d'utilisation, Galliker peut évaluer les enregistrements sous forme anonyme ou pseudonyme.

L'évaluation sous pseudonyme ne se fait que par échantillonnage. Galliker doit ici indiquer le calendrier et la période pendant laquelle l'échantillonnage est effectué. Pour garantir l'anonymat et le pseudonymat, Galliker gardera le nombre de personnes examinées suffisamment grand et conservera les procès-verbaux séparés physiquement et fonctionnellement de la liste de correspondance.

Si l'évaluation anonyme ou pseudonyme fait naître un soupçon d'abus ou si un abus est constaté, les évaluations du protocole sont évaluées nominativement en les reliant à la liste de correspondance. Par abus, on entend une violation du règlement d'utilisation.

Si un soupçon d'abus ne se confirme pas, notre entreprise met immédiatement fin à l'exploitation nominative de la journalisation.

Seul le responsable de la protection des données et l'équipe d'IT-Network Services ont accès aux enregistrements de surveillance et peuvent procéder à une évaluation nominative de la journalisation.

Si un délit est constaté ou soupçonné par l'évaluation des enregistrements ou par d'autres indications, Galliker sécurise les enregistrements correspondants. Galliker se réserve le droit de porter plainte contre le collaborateur concerné. La décision de porter plainte ou non appartient à la direction. Il n'est pas obligatoire de porter plainte. Il est toutefois recommandé de porter plainte, du moins en ce qui concerne les délits officiels, afin d'éviter le risque de complicité.

La suite de la procédure est du ressort de l'autorité de justice pénale compétente. Notre entreprise s'engage à traiter le résultat de l'enquête de manière confidentielle vis-à-vis de tiers non autorisés, en particulier vis-à-vis des autres collaborateurs.

Galliker s'engage à utiliser en premier lieu des mesures de protection techniques contre les abus et les dommages techniques. Galliker adapte régulièrement les mesures de protection techniques à l'état le plus récent de la technique. L'adaptation a également lieu après un incident technique. Ce n'est que si un abus ne peut pas être évité malgré les mesures de protection techniques qu'une évaluation personnelle des protocoles Internet et e-mail peut être effectuée. Galliker renonce à l'utilisation de programmes d'espionnage.

Si un dysfonctionnement de l'infrastructure informatique se manifeste malgré les mesures de protection techniques, les journaux peuvent être utilisés pour en rechercher la cause.

Si le trouble est à l'origine d'un abus, le travailleur identifié peut être sanctionné.

Si d'autres indices font naître un soupçon d'abus ou si un abus est constaté, les procès-verbaux correspondants ou leurs évaluations peuvent être consultés si nécessaire. En cas d'abus avéré, des sanctions relevant du droit du travail peuvent être prises.

11.5.2 Accès aux e-mails et aux documents relevants

De même, une évaluation peut avoir lieu en particulier des e-mails et des données, indépendamment du fait qu'ils soient déjà archivés ou non, si ceux-ci sont nécessaires à des fins de conservation des preuves, en particulier s'ils permettent de faire valoir des droits juridiques contre des tiers ou s'ils servent à se défendre contre des droits juridiques de tiers vis-à-vis de Galliker (comme des procédures civiles, pénales ou administratives). Si des actes punissables d'un collaborateur sont révélés à cette occasion, Galliker peut déposer une plainte pénale. Les principes mentionnés au paragraphe 11.5.1 s'appliquent. En outre**,** la ⇨ **directive d'archivage et de suppression** s'applique.

11.5.3 Utilisation à des fins privées

Le collaborateur a le droit, dans le cadre de l'accord en vigueur, d'utiliser occasionnellement son infrastructure IT autorisée à des fins privées en utilisant des adresses électroniques privées, à condition que cela ne nuise pas à l'activité du collaborateur pendant les heures de travail et que cela n'entraîne pas de frais supplémentaires pour Galliker.

Galliker entend par utilisation privée occasionnelle et donc raisonnable le fait que les collaborateurs passent par exemple de temps en temps de brefs appels téléphoniques nationaux, qu'ils envoient ou lisent de temps à autre des e-mails privés identifiés comme tels ou qu'ils consultent parfois brièvement une information sur Internet. Dans des circonstances particulières, les collaborateurs peuvent convenir d'autres arrangements avec leurs supérieurs. Si des e-mails ou d'autres données ne sont pas marqués comme privés, ils peuvent faire l'objet d'un accès aux e-mails et aux données conformément au paragraphe 11.5.1 et le collaborateur y consent expressément en utilisant l'infrastructure IT.

Galliker peut notamment vérifier les éventuels décomptes pour s'assurer que le cadre approprié a été respecté (en particulier pour les appareils mobiles).

11.6 Déclaration de consentement

Le règlement d'utilisation IT fait partie intégrante du contrat de travail. En signant le contrat de travail, tous les collaborateurs confirment qu'ils ont pris connaissance du contenu de ce document et qu'ils l'approuvent, en particulier en ce qui concerne la consignation de l'utilisation des moyens de communication électroniques pour des raisons d'exploitation et de sécurité ainsi que l'accès aux e-mails et aux documents pertinents qui ne sont pas désignés comme privés. En signant le contrat de travail, les collaborateurs confirment en outre qu'ils sont d'accord avec le respect des directives informatiques conformément au règlement d'utilisation IT.

12. Sécurité des appareils mobiles

12.1 Responsabilité

Le collaborateur est responsable de la sécurité de l'infrastructure IT qu'il utilise à des fins professionnelles, en particulier des appareils mobiles et privés.

Les appareils mobiles ne doivent pas être laissés sans surveillance (même lors de congrès, dans la voiture, etc.). Dans les régions dangereuses du monde, les appareils mobiles ne doivent pas être utilisés en public, afin de ne pas créer un danger pour la vie et l'intégrité corporelle.

L'infrastructure IT utilisée pour l'exploitation ne doit pas être remise à des personnes connues ou inconnues pour utilisation.

En cas de perte de l'appareil mobile, ne serait-ce que pour quelques heures, il faut en informer immédiatement les services IT afin d'empêcher des tiers d'accéder aux données Galliker.

Le scanner antivirus installé par défaut assure une sécurité suffisante au sein de l'entreprise. La prudence est de mise avec les pièces jointes (données et programmes) d'origine interne ou externe à l'entreprise ou provenant d'une source non sûre.

La prudence est de mise lorsque l'on surfe sur des sites web ou que l'on traite des e-mails et des données. Il convient d'éviter les sites qui n'ont pas d'intérêt commercial ou qui présentent des failles de sécurité évidentes.

La saisie de données d'utilisateur sur de tels sites peut entraîner la perte de données ou du compte et contribuer à causer des dommages aux clients ou à Galliker. Si un tel incident se produit, il doit être immédiatement signalé aux services informatiques.

Les e-mails qui semblent suspects, qui proviennent d'expéditeurs inconnus et auxquels on ne peut attribuer aucune pertinence commerciale doivent être signalés aux services informatiques.

12.2 Travaux d'entretien ou de réparation et élimination par des organismes agréés

Si des travaux de maintenance ou de réparation doivent être effectués sur l'appareil mobile (p. ex. remplacement d'un écran défectueux) ou si celui-ci doit être éliminé, ces travaux ne peuvent être effectués que par un centre de réparation autorisé à cet effet par les services IT de Galliker. Cela vaut pour les appareils privés comme pour les appareils professionnels.

La raison de ce règlement est que l'appareil est mis entre les mains de personnes dont la fiabilité n'est pas connue. Ces personnes pourraient très facilement apporter des modifications à votre appareil mobile (par exemple, installer des logiciels espions ou du matériel supplémentaire sur leur appareil) dans le but d'espionner ou de modifier vos mots de passe et toutes les communications que vous effectuez via votre appareil mobile (par exemple, les virements bancaires) sans que vous ne puissiez le détecter.

12.3 Précautions à prendre avant les travaux d'entretien ou de réparation, le remplacement et l'élimination

Avant de remettre l'appareil au service de réparation, il faut effacer toutes les données ainsi que les comptes d'utilisateurs professionnels, si cela est possible. En cas de doute, il convient de s'adresser aux services IT de Galliker.

13. Assistance générale aux utilisateurs

L'assistance générale aux utilisateurs (p. ex. réglages des appareils, utilisation générale des appareils, brèves instructions) n'est fournie qu'aux collaborateurs autorisés et uniquement pour les appareils et systèmes d'exploitation internes. Le support général aux utilisateurs peut être contacté via Galliker IT-Services.

14. Réseau et accès à Internet

L'accès au réseau câblé est disponible dans les bureaux de Galliker.

Les appareils des clients, des intervenants, des collaborateurs externes ou les PC privés des collaborateurs de Galliker ne doivent pas être connectés au réseau de domaine de Galliker. Les services IT de Galliker Services veillent à ce qu'un réseau alternatif soit disponible pour les appareils qui ne peuvent pas être connectés au réseau de domaine de Galliker (par exemple dans les espaces publics comme les salles de réunion).

L'accès à Internet via des réseaux WLAN ne doit se faire que par l'intermédiaire de fournisseurs de confiance (providers) et uniquement au moyen d'un VPN.

Une connexion WLAN à Internet ne peut être établie que si le logiciel de sécurité lié à l'appareil (pare-feu, antivirus, etc.) fonctionne correctement et si la connexion WLAN dispose de mesures de sécurité suffisantes (protection par mot de passe ou par certificat).

15. Formation des collaborateurs

Les collaborateurs connaissent l'importance de la sécurité informatique ou de la protection des informations dans leur travail quotidien. Ils sont régulièrement instruits à ce sujet par leurs supérieurs et par des formations périodiques des services IT de Galliker.

16. Entrée en vigueur

Ce règlement entre en vigueur le 01 juin 2024 (remplace la version du 24 octobre 2023).

Altishofen, 01.06.2024 La direction