Charte d'utilisation du système d'information et de communication de la société Bruno SIEBERT S.A.

Préambule

L'entreprise Bruno SIEBERT S.A. met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique.

Les salariés, dans l'exercice de leurs fonctions, sont conduits à accéder aux moyens d'information et de communication mis à leur disposition et à les utiliser.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles.

Dans un but de transparence à l'égard des utilisateurs et de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, la présente charte, associée au règlement intérieur, pose les règles relatives à l'utilisation de ces ressources.

Article 1. Champ d'application

1.1 Utilisateurs concernés

La présente charte s'applique à l'ensemble des personnes ayant accès au système d'information et de communication de l'entreprise (on les nommera « utilisateur(s) »), quel que soit leur statut, y compris les mandataires sociaux, le personnel permanent, le personnel intérimaire, les stagiaires, les visiteurs occasionnels et le personnel travaillant avec la société Bruno SIEBERT S.A. (employés de sociétés prestataires, sous-traitants, fournisseurs, clients,…).

Les salariés veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

1.2 Système d'information et de communication

Le système d'information et de communication de l'entreprise est notamment constitué des éléments suivants : ordinateurs (fixes et portables), périphériques, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones (fixes et portables), fax, logiciels, fichiers, données et bases de données, système de messagerie, internet, abonnements à des services interactifs (exemple : sites payants), informations, applications, machine à affranchir.

B.S

La composition du système d'information et de communication est indifférente à la propriété sur les éléments qui le composent.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés connecté au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'entreprise.

1.3 Accès aux outils informatiques et aux ressources de communication

L'accès aux outils informatiques et aux ressources de communication est soumis à l'autorisation préalable du responsable hiérarchique ou à toute personne habilitée par lui. L'utilisation des outils informatiques et des ressources de communication n'est autorisée que dans le cadre exclusif de l'activité professionnelle de l'utilisateur et durant le temps de travail contractuel de celui-ci. Ces autorisations sont strictement personnelles et ne peuvent être cédées à des tiers qu'en cas de force majeure et sous réserve préalable de l'autorisation de la hiérarchie. Elles peuvent être retirées à tout moment sur décision unilatérale de la hiérarchie.

Toute autorisation prend fin lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifiée.

Article 2. Confidentialité des paramètres d'accès

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiants, mots de passe).

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs.

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information. L'utilisateur ne doit ni utiliser ni essayer d'utiliser des mots de passe autres que le sien. Il ne doit en aucun cas masquer ou essayer de masquer sa véritable identité.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par le responsable informatique afin de recommander les bonnes pratiques en la matière (cf. Note de Service du 18 Mai 2015).

BS

Article 3. Protection des ressources sous la responsabilité de l'utilisateur

L'entreprise met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. A ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

Le responsable informatique est responsable du contrôle du bon fonctionnement du système d'information et de communication. Il veille à l'application des règles de la présente charte en concertation avec la direction. Le responsable informatique est assujetti à une obligation de confidentialité sur les informations qu'il est amené à connaître.

L'utilisateur est responsable, quant à lui, des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection desdites ressources, en faisant preuve de prudence.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

En cas d'accès au système d'information avec du matériel n'appartenant pas à l'entreprise (assistants personnels, supports amovibles - exemple : clés USB -, ...), il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité. Un tel accès requiert l'autorisation préalable du responsable hiérarchique et du responsable informatique.

L'utilisateur doit effectuer des enregistrements réguliers des fichiers dont il dispose sur le matériel mis à sa disposition pour assurer la protection de ses informations.

Le responsable informatique doit quant à lui effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition pour assurer la protection des informations.

L'utilisateur doit éviter d'installer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'entreprise. Il doit dans tous les cas en alerter sa hiérarchie et le responsable informatique.

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

B.S

L'utilisateur doit signaler tout dysfonctionnement du système d'information et de communication ou tout problème pouvant nuire au bon niveau de sécurité (exemple : alerte virale, problème/faille système, mauvaise gestion des protections, logiciels suspects, etc.) à sa hiérarchie et au responsable informatique dans les meilleurs délais. Il ne doit pas déployer des moyens informatiques sans l'accord de ceux-ci.

Article 4. Accès à internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le responsable informatique. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et soit en corrélation avec les fonctions exercées ou les missions à mener.

Sauf autorisation préalable de la direction, la contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée (conversation en ligne), blogs, sites, sites payants est interdite.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de l'entreprise, y compris sur internet.

Article 5. Messagerie électronique

La messagerie électronique est un moyen d'amélioration de la communication au sein des entreprises et avec les tiers. A sa demande, un salarié peut disposer, pour l'exercice de son activité professionnelle et après validation de sa hiérarchie, d'une adresse de messagerie électronique attribuée par le responsable informatique.

Le courrier électronique est une véritable correspondance et doit être traité avec autant de rigueur qu'une lettre ou un fax. Comme la lettre ou le fax, le courrier électronique est à usage strictement professionnel.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer leur hiérarchie et le responsable informatique des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

5.1 Conseils généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter

13.5

l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l'entreprise et/ou de l'utilisateur.

L'envoi de messages électroniques à des tiers obéit aux mêmes règles que l'envoi de correspondances postales, en particulier en termes d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à l'autorité hiérarchique.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et leur qualité à recevoir communication des informations transmises.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel.

Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants sont envoyés avec un accusé de réception. Ils doivent, le cas échéant, être doublés par des envois postaux.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

Pour toute absence supérieure à 1 jour, l'utilisateur devra mettre en place un répondeur automatique (cf. Note de Service du 19 Mai 2015).

5.2 Limites techniques

La taille, le nombre et le type des pièces jointes peuvent être limités par le responsable informatique pour éviter l'engorgement du système de messagerie.

5.3 Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

Les messages envoyés doivent être signalés par la mention « PERSONNEL » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé « PERSONNEL ».

135

Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « PERSONNEL ».

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

5.4 Suppression de compte

En cas de départ définitif d'un salarié, son compte de messagerie sera placé sur répondeur pendant une durée de 3 mois.

Passé ce délai, le compte de messagerie sera supprimé. L'entreprise se réserve le droit de consulter les messages à caractère professionnel avant la suppression du compte.

5.5 Utilisation de la messagerie pour la communication destinée aux institutions représentatives du personnel

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel.

Article 6. Contrôle des activités

6.1 Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (« *logs* »), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives:

— à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications/suppressions de fichiers,
— aux connexions entrantes et sortantes au réseau interne, à la messagerie et à internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le téléchargement de fichiers.

13 S

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

6.2 Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le responsable informatique et/ou par la direction, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateur(s).

Lorsque le contrôle porte sur les fichiers d'un utilisateur, et sauf risque ou événement particulier, le responsable informatique et/ou la direction ne peut/peuvent ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou avec l'autorisation expresse du salarié d'un représentant du personnel (CE, CHSCT).

Le contenu des messages à caractère personnel des utilisateurs (tels que définis à l'article 5.3) ne peut en aucun cas être contrôlé par le responsable informatique/la direction.

Article 7. Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

Article 8. Information des salariés

La présente charte est affichée publiquement en annexe du règlement intérieur.

Le responsable informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des Nouvelles Technologies de l'Information et de la Communication (NTIC). Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

Des opérations de communication internes seront organisées, de manière régulière, afin d'informer les salariés sur les pratiques d'utilisation des Nouvelles Technologies de l'Information et de la Communication (NTIC) recommandées.

13.5

Chaque utilisateur doit s'informer sur les techniques de sécurité et veiller à maintenir son niveau de connaissance en fonction de l'évolution technologique.

Article 9. Rappel des principales lois françaises en vigueur

La présente charte s'inscrit dans le cadre des dispositions législatives et règlementaires, en particulier dans le domaine de la sécurité informatique :

-Loi n° 78-17 du 6/1/78 dite « informatique et liberté » complétée par la loi du 06/08/2004

-Articles 226-16 à 226624 du Code Pénal

-Loi n° 85-660 du 03/07/1985 sur les droits d'auteur

-Loi n° 94-361 du 10/05/1994

-Loi n° 98-536 du 01/07/1998

-Code de la Propriété Intellectuelle

-Loi n° 88-19 du 05.01.1988 relative à la fraude informatique

-Loi n° 91-646 du 10/07/1991 relative au secret des correspondances émises par voie des télécommunications.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose à des poursuites disciplinaires et pénales, prévues par les textes législatifs et réglementaires en vigueur.

Article 10. Entrée en vigueur

La présente charte est applicable à compter du 17 août 2015.

Elle a été adoptée après information et consultation du comité d'hygiène et de sécurité (CHSCT) le 16 juin 2015 et du comité d'entreprise le 23 juin 2015.

13.5

Ergersheim, le 18 Mai 2015

NOTE DE SERVICE

De la part du Service Informatique

À l'attention de l'ensemble des personnes ayant accès au système d'information et de communication de l'entreprise Bruno SIEBERT S.A.

Objet :
Confidentialité des paramètres d'accès au système d'information : procédure de changement de mot de passe

Mesdames, Messieurs,

Pour des raisons de sécurité, les mots de passe d'ouverture de session Windows sont révoqués tous les 60 jours. Il est vivement conseillé de choisir un mot de passe composé de chiffres et de lettres soit, au minimum, 8 caractères. Ce dernier est strictement personnel et ne doit jamais être communiqué.
Nous vous rappelons aussi qu'il est très important de penser à verrouiller votre poste quand vous vous absentez. Pour cela, tenez la touche en forme de drapeaux enfoncée puis appuyez sur L.

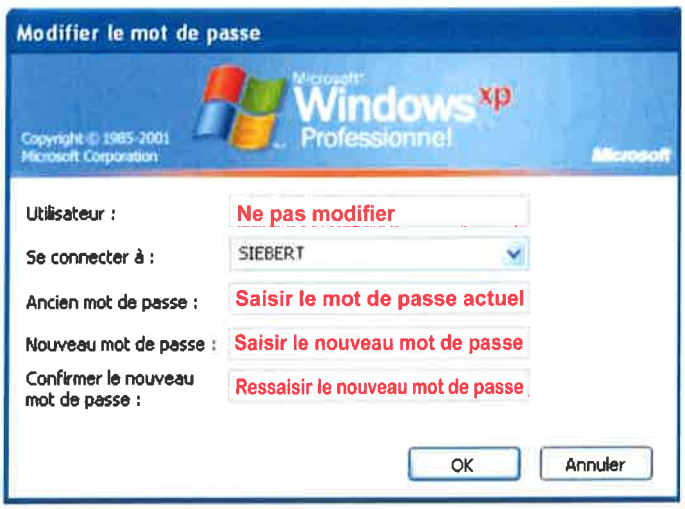
Mais il vous est aussi possible de changer votre mot de passe à tout moment.

Pour cela :

Étape 1 : Appuyez sur Ctrl+Alt+Suppr pour atteindre l'écran d'accueil puis cliquez sur « Modifier le mot de passe… »

Étape 2 : Votre ancien mot de passe vous est demandé, puis le nouveau. Confirmez ce nouveau mot de passe et validez l'opération en pressant sur la touche Entrée.

C'est terminé, un message confirmant le changement de mot de passe apparaît.



Cordialement,

Vincent Schwartz

13.2

Ergersheim, le 19 mai 2015

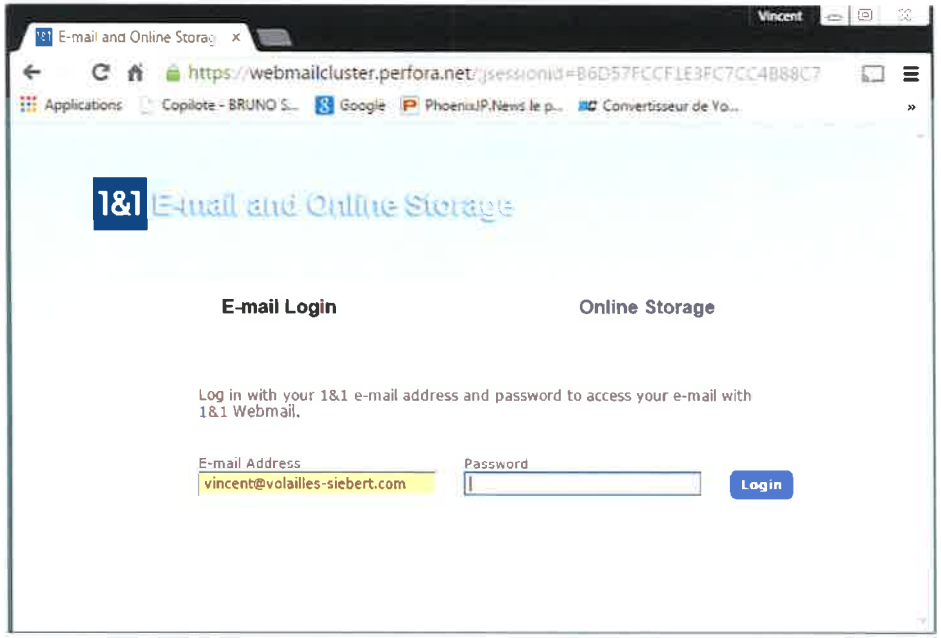
NOTE DE SERVICE

De la part du Service Informatique

À l'attention de l'ensemble des personnes ayant accès au système
D'information et de communication de l'entreprise Bruno SIEBERT S.A.

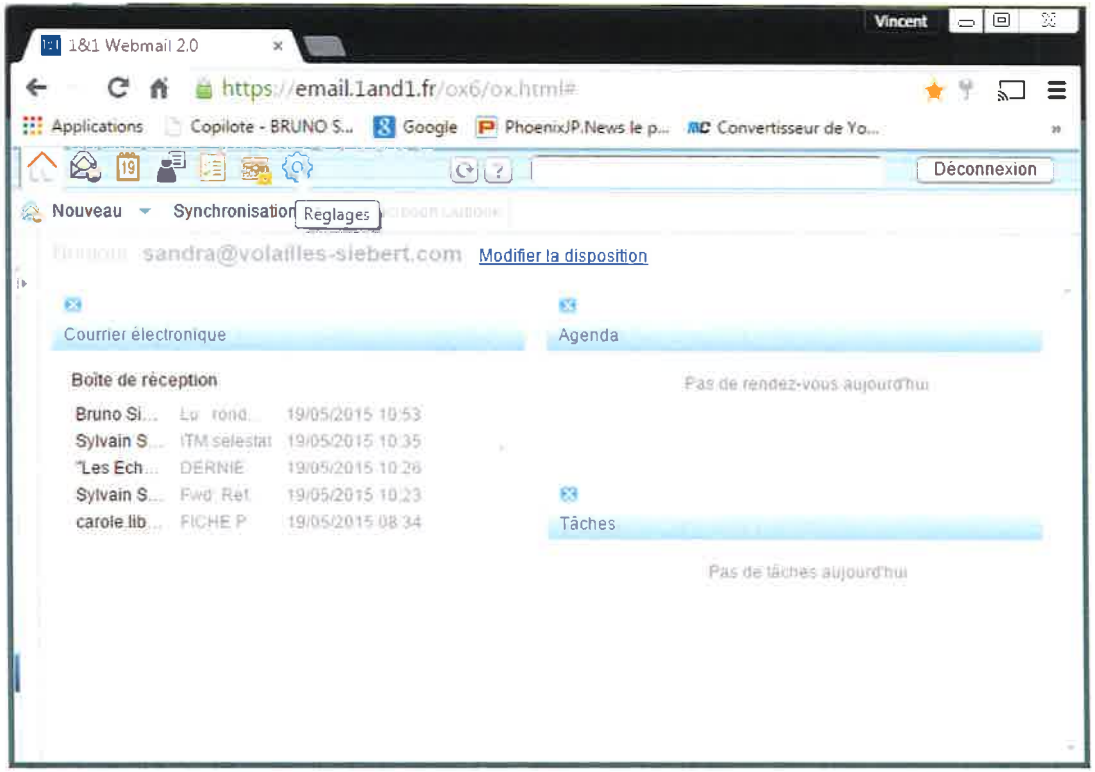
Objet :
Mise en place d'un répondeur automatique (message d'absence e-mail)

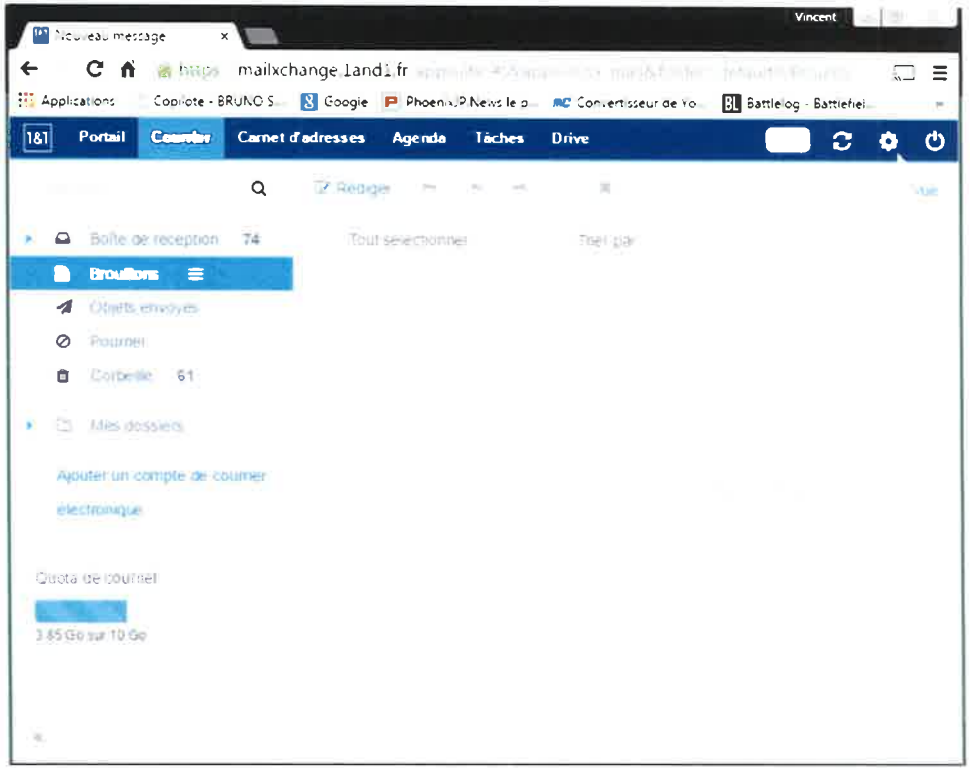
-Ouvrir le navigateur web,
-Aller sur le site https://email.1and1.com,
-S'identifier à l'aide de son adresse e-mail et de son mot de passe (ce dernier vous sera communiqué par le Responsable Informatique sur demande),

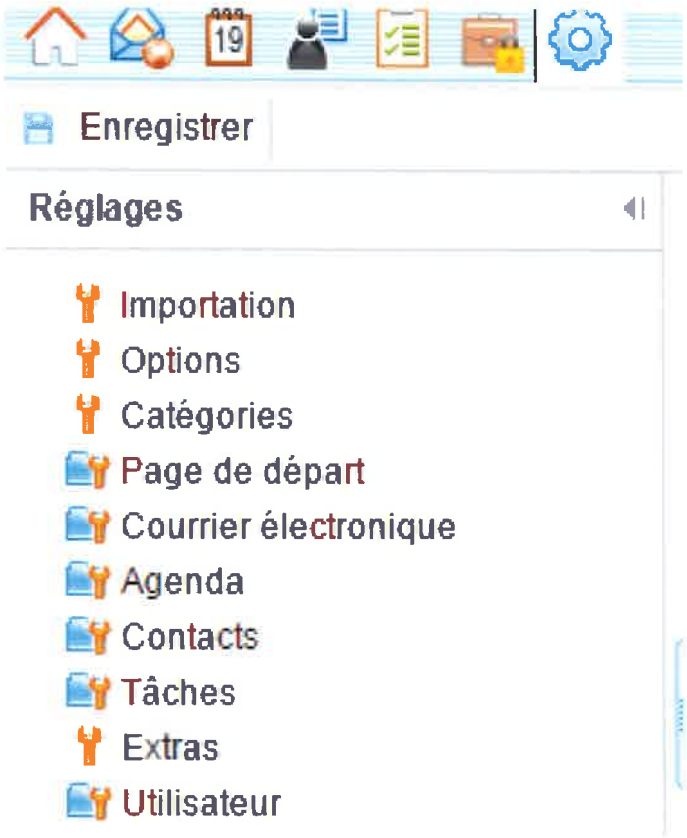


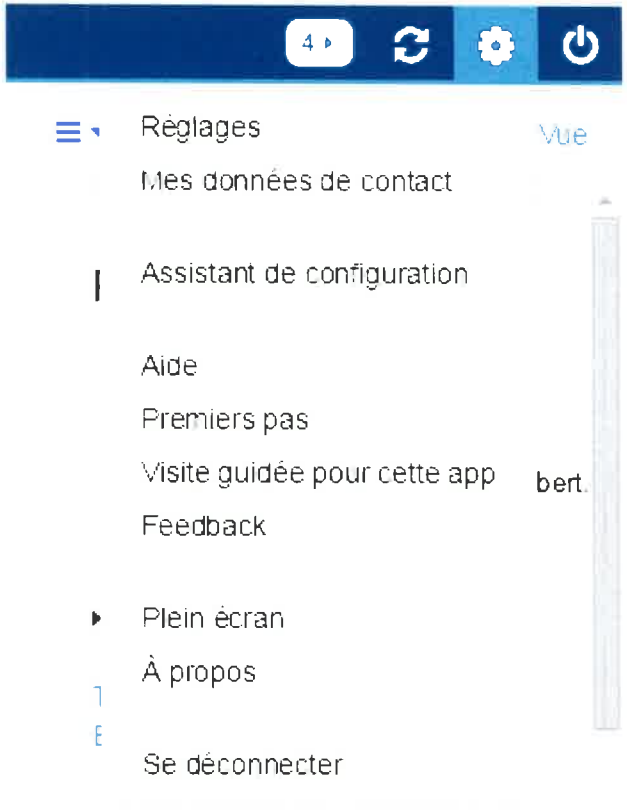
13.5

-Cliquer sur l'image en forme de roue dentée « Réglages » ou selon le cas,
-Puis cliquer sur « Extras » ou « Réglages » selon le cas,

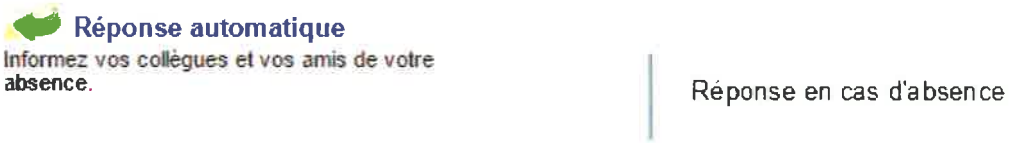








-Patienter quelques secondes puis cliquer sur « Réponse automatique » ou « Réponse en cas d'absence » selon le cas,
-Enfin, cliquer sur « Activer », remplir les différents champs et valider si demandé.



ATTENTION : Pour désactiver le répondeur automatique, répéter toute la procédure et cliquer sur « Arrêt » ou décocher la case « Activer ».

Cordialement,

Vincent Schwartz