

REGLEMENT INTERIEUR
EN APPLICATION DES ARTICLES L.1311-1 ET SUIVANTS
DU CODE DU TRAVAIL

PREAMBULE

Il est rappelé en préambule que la convention collective applicable au sein du Grand Port Maritime de Marseille est la Convention collective nationale unifiée « Ports et Manutention ».

La notion « d'employeur ou son représentant » s'entend de toute personne ayant autorité sur des salariés dans une relation hiérarchique.

Ceci étant exposé, il est convenu ce qui suit.

1. OBJET

Le présent règlement intérieur est pris en application des articles L.1311-1 et suivants du Code du travail. Conformément à la loi, il fixe :

- les règles relatives aux harcèlements sexuel, moral et aux agissements sexistes
- les règles relatives à l'hygiène et à la sécurité au sein du Grand Port Maritime de Marseille
- les règles générales et permanentes relatives à la discipline
- les procédures et sanctions disciplinaires ainsi que les dispositions relatives aux droits de la défense des salariés

Sont annexé au présent règlement :

- le code de conduite relatif à la corruption et au trafic d'influence conformément à la loi n° 2016-1691 du 9 décembre 2016.
- la charte de l'utilisateur.

2. CHAMP D'APPLICATION

Le présent règlement s'applique à tous les agents du GPMM sans restriction ni réserve.

Il s'applique sur l'ensemble des sites et dans tous les lieux composant le Grand Port Maritime de Marseille (y compris quais, entrepôts, cantines, aires de stationnement...).

Les personnes mises à disposition par une société de travail temporaire, les personnes effectuant un stage dans l'établissement ainsi que les salariés d'entreprises extérieures travaillant sur le Port pour le compte du Grand Port Maritime de Marseille, doivent se conformer aux termes du présent règlement intérieur ainsi qu'à ceux de la Charte de l'Utilisateur qui y est annexée.

Des dispositions spéciales pourront éventuellement être établies pour fixer les conditions applicables à une catégorie de personnel ou à une division de l'établissement, conformément à l'article L.1311-2 du Code du travail.

CHAPITRE I

REGLES RELATIVES AUX HARCELEMENTS SEXUEL, MORAL ET AUX AGISSEMENTS SEXISTES

3. HARCELEMENT SEXUEL

Le harcèlement sexuel est défini par l'article 222-33 du code pénal :

« I. - Le harcèlement sexuel est le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle ou sexiste qui soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante.

L'infraction est également constituée :

1° Lorsque ces propos ou comportements sont imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée ;

2° Lorsque ces propos ou comportements sont imposés à une même victime, successivement, par plusieurs personnes qui, même en l'absence de concertation, savent que ces propos ou comportements caractérisent une répétition.

II. - Est assimilé au harcèlement sexuel le fait, même non répété, d'user de toute forme de pression grave dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers.

III. - Les faits mentionnés aux I et II sont punis de deux ans d'emprisonnement et de 30 000 € d'amende.

Ces peines sont portées à trois ans d'emprisonnement et 45 000 € d'amende lorsque les faits sont commis :

1° Par une personne qui abuse de l'autorité que lui confèrent ses fonctions ;

2° Sur un mineur de quinze ans ;

3° Sur une personne dont la particulière vulnérabilité, due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, est apparente ou connue de leur auteur ;

4° Sur une personne dont la particulière vulnérabilité ou dépendance résultant de la précarité de sa situation économique ou sociale est apparente ou connue de leur auteur ;

5° Par plusieurs personnes agissant en qualité d'auteur ou de complice ;

6° Par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique ;

7° Alors qu'un mineur était présent et y a assisté ;

8° Par un ascendant ou par toute autre personne ayant sur la victime une autorité de droit ou de fait. »

Selon les dispositions des articles L.1153-1 et suivants du Code du travail, aucun salarié ne doit subir des faits :

- Soit de harcèlement sexuel, constitué par des propos ou comportements à connotation sexuelle répétés qui soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante ;
- Soit assimilés au harcèlement sexuel, consistant en toute forme de pression grave, même non répétée, exercée dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers.

Par ailleurs, aucun salarié, aucune personne en formation ou en stage, aucun candidat à un recrutement, à un stage ou à une formation en entreprise ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat pour avoir subi ou refusé de subir des faits de harcèlement sexuel tels que définis à l'article L. 1153-1, y compris, dans le cas mentionné au 1° du même article, si les propos ou comportements n'ont pas été répétés.

Aucun salarié, aucune personne en formation ou en stage ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire pour avoir témoigné de faits de harcèlement sexuel ou pour les avoir relatés.

Toute disposition ou tout acte contraire aux dispositions susvisées est nul.

Tout salarié ayant procédé à des faits de harcèlement sexuel est passible d'une sanction disciplinaire.

4. HARCELEMENT MORAL

L'article 222-33-2 du Code pénal dispose que « le fait de harceler autrui par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel, est puni de deux ans d'emprisonnement et de 30 000 € d'amende. »

Selon les dispositions des articles L.1152-1 et suivants du Code du travail, aucun salarié ne doit subir les agissements répétés de harcèlement moral qui ont pour objet ou pour effet une dégradation de ses conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel.

Aucun salarié, aucune personne en formation ou en stage ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat pour avoir subi ou refusé de subir des agissements répétés de harcèlement moral ou pour avoir témoigné de tels agissements ou les avoir relatés.

Toute disposition ou tout acte contraire aux dispositions susvisées est nul.

Par ailleurs, tout salarié ayant procédé à des agissements de harcèlement moral est passible d'une sanction disciplinaire.

5. AGISSEMENTS SEXISTES

Selon les dispositions de l'article L. 1142-2-1 du Code du travail, nul ne doit subir d'agissement sexiste, défini comme tout agissement lié au sexe d'une personne, ayant pour objet ou pour effet de porter atteinte à sa dignité ou de créer un environnement intimidant, hostile, dégradant, humiliant ou offensant.

Est passible d'une sanction disciplinaire tout salarié ayant procédé aux agissements précédemment définis.

CHAPITRE II

REGLES RELATIVES À L'HYGIENE ET À LA SECURITE

Le personnel est tenu d'appliquer et de respecter les mesures d'hygiène et de sécurité édictées dans le cadre des dispositions légales et réglementaires en vigueur, les consignes générales et particulières de sécurité propre à l'établissement ainsi que les prescriptions de la médecine du travail.

6. VISITE MEDICALE

Tout salarié doit se soumettre au suivi médical prévu par les textes réglementaires applicables telles que notamment : visite d'information et de prévention, visite périodique, examen médical d'aptitude, visite de reprise du travail, visite à la demande de l'employeur, ainsi qu'à tout examen ou test complémentaire jugé nécessaire par le médecin du travail ou l'équipe pluridisciplinaire de santé au travail en fonction du poste de travail occupé par le salarié.

7. PREVENTION DES ACCIDENTS

Pour l'exécution de leur travail, les salariés ont l'obligation de respecter toutes les consignes et prescriptions qui leur sont données par l'employeur ou son représentant ou inhérentes à leurs qualifications, habilitations ou formations professionnelles, notamment les instructions relatives à la sécurité.

Il appartient à chaque responsable hiérarchique de s'assurer du respect par les salariés placés sous sa responsabilité de ces consignes et instructions.

Il incombe à chaque salarié de prendre soin de sa sécurité et de sa santé, ainsi que de celles des autres personnes concernées par ses agissements.

Chaque salarié doit veiller à sa sécurité personnelle et utiliser tous les moyens de protection collective ou individuelle, adaptés à son travail, mis à sa disposition (tels que casque, lunettes, gants, masques à cartouches, vêtements de travail, chaussures et harnais de sécurité...) et respecter strictement les consignes d'utilisation de ces moyens de protection.

Sauf dérogations particulières établies par l'employeur ou son représentant, et sauf mise en œuvre de mesures de sécurité spécifiques, il est interdit d'utiliser des moyens, méthodes, appareils susceptibles d'être à l'origine d'un incendie ou d'une explosion dans tous les locaux, emplacements, installations, où ces risques sont présents et/ou font l'objet d'une signalisation adaptée.

Tout membre du personnel est tenu de prendre connaissance des consignes générales en cas d'incendie et de s'y conformer en cas de nécessité. Tout membre du personnel est également tenu de participer aux exercices de sauvetage et d'évacuation organisés dans l'établissement.

Il est interdit d'enlever ou de neutraliser les moyens de lutte contre l'incendie, de limiter leur accès, de les déplacer ou de les employer à un autre usage. Toute anomalie devra

être signalée à la hiérarchie. Il est interdit d'encombrer, de condamner, de rendre inaccessible les issues et couloirs de circulation des locaux et installations.

D'une façon générale, toute anomalie ou toute situation de danger devra être signalée à l'employeur ou à son représentant.

Conformément aux articles L.4131-1 et suivants du Code du travail, tout salarié a le droit de se retirer d'une situation de travail dont il a un motif raisonnable de penser qu'elle présente un danger grave et imminent pour sa vie ou sa santé, résultant par exemple d'une défectuosité d'un système de protection. L'exercice du droit de retrait ne doit pas créer pour autrui une nouvelle situation de danger grave et imminent.

L'exercice du droit de retrait est subordonné à l'existence d'un danger grave et imminent, ces deux conditions devant être simultanées :

- adjectif « grave » : « tout danger susceptible de produire un accident ou une maladie entraînant la mort ou paraissant devoir entraîner une incapacité permanente ou temporaire prolongée ».
- adjectif « imminent » : « tout danger susceptible de se réaliser brutalement dans un délai rapproché ».

8. EQUIPEMENTS DE TRAVAIL, OUTILLAGE, MACHINES

Il est rappelé au préalable que les équipements de travail notamment les engins, matériels, outillage et machines du Port ne peuvent être utilisés qu'à des fins professionnelles, et non à des fins personnelles.

La prévention des risques d'accidents impose l'obligation pour chaque salarié de conserver en bon état de marche, équipements de travail, engins, matériels, outillage et machines et plus généralement tout matériel qui lui est confié en vue de l'exécution de ses tâches de travail.

Les salariés n'ayant pas reçu la formation spécifique et/ou la délivrance d'une autorisation de conduite ne peuvent conduire les équipements de travail, engins et machines pour lesquels la réglementation l'impose.

Il est rappelé que les interventions de maintenance, préventive ou curative ou de réglage sur tout équipement ou installation, doivent impérativement être effectuées par du personnel formé et dûment habilité, dans la mesure où ces interventions requièrent une habilitation réglementaire, et dans le respect des procédures prévues pour ces interventions.

Les salariés doivent utiliser les équipements de travail, engins, matériels, outillage, machines mis à leur disposition pour les besoins de leur activité professionnelle, conformément à leur destination et aux conditions normales d'emploi, dans le strict respect des prescriptions en matière de sécurité et des notices d'utilisation lorsqu'elles existent. Ils doivent signaler immédiatement à l'employeur ou son représentant les défaillances ou défectuosités constatées.

Lorsque le travail d'exécution comporte également l'entretien ou le nettoyage des machines ou engins, le salarié est tenu d'y consacrer le temps nécessaire.

Il est rappelé que sont interdits, l'enlèvement, la neutralisation, la détérioration d'un dispositif de protection des machines et équipements, ainsi que la détérioration des outillages et installations qui pourraient avoir des incidences sur la sécurité des

personnes et des biens, sauf dans le cas de mise en place d'un mode de marche dégradé identifié et ayant fait l'objet d'une procédure formalisée.

L'accès aux équipements de travail, engins et outillage, réglementé et réservé aux personnes autorisées, doit se faire obligatoirement par les installations prévues à cet effet. Il est notamment interdit d'accéder aux cabines de grues, et autres engins, ou d'en descendre, autrement que par les moyens prévus à cet effet.

L'accès aux locaux techniques est réservé aux personnels autorisés.

9. INSTALLATIONS ELECTRIQUES

L'accès aux locaux électriques et/ou les interventions sur les installations électriques sont réservés aux seuls salariés habilités à cet effet.

Les salariés habilités doivent procéder aux manœuvres, travaux, consignations et toutes opérations relatives aux installations électriques dans le respect des prescriptions de sécurité mis à disposition, notamment celles définies par le recueil d'instructions de sécurité électrique pour les ouvrages UTE C 18-510.

Les salariés non habilités en matière électrique ne peuvent intervenir sur une installation électrique.

10. SUBSTANCES ILLICITES

Il est interdit de pénétrer dans l'établissement sous l'emprise de produits stupéfiants ou de substances illicites. De même, l'introduction, l'usage et/ou le stockage de tout produit illicite sont formellement interdits au sein de l'établissement.

Lorsque l'employeur ou son représentant se trouve confronté à un agent présentant des troubles manifestes, il doit alors prendre toutes dispositions pour que cet agent ne soit ni à l'origine de, ni exposé à quelque risque que ce soit du fait de son état.

Ces dispositions doivent être d'autant plus efficaces lorsque l'agent exerce des fonctions nécessitant l'intégrité de ses capacités, mentales et physiques : conduite d'engin ou de véhicule, manipulations sur des produits dangereux, travaux mécaniques, travaux en hauteur, travaux d'ordre électrique, interventions de toutes natures sur navires, etc.

Pour ce faire, l'employeur ou son représentant doit faire en sorte d'écarter l'agent des risques auxquels il pourrait se trouver exposé dans le cadre de son poste de travail, en lui proposant un temps de repos, notamment sur place, dans une salle de repos ou un bureau, ou en le faisant accompagner chez le médecin du travail ou un médecin, qui pourra prescrire tout examen médical complémentaire ou test de dépistage qu'il jugerait utile.

Durant cette phase, l'agent pourra demander à être assisté d'un membre du personnel de son choix, disponible au regard des nécessités de service.

Eu égard au respect de l'individu, l'application de cette procédure doit revêtir un caractère de discrétion absolue.

11. BOISSONS ALCOOLISEES

Il est interdit d'introduire, stocker, distribuer ou consommer sur les lieux de travail, toutes boissons alcoolisées, en dehors d'une consommation modérée pour les personnes qui n'occupent pas de poste à risque ou de sécurité pendant le temps de repas des boissons alcoolisées énoncées à l'article R.4228-20 du Code du Travail

Il est interdit à tout salarié, ainsi qu'aux membres du personnel d'entreprises intervenantes ou toute autre personne, de pénétrer ou de demeurer en état d'ivresse dans l'enceinte de l'établissement.

Conformément à l'article R.4228-21 du Code du Travail, il est interdit de laisser entrer ou séjourner dans les lieux de travail des personnes en état d'ivresse.

L'employeur ou son représentant peut se trouver confronté à un agent présentant des signes extérieurs d'alcoolisation. Il doit alors prendre toutes dispositions pour que cet agent ne soit ni à l'origine de, ni exposé à quelque risque que ce soit du fait de son état.

Ces dispositions doivent être d'autant plus efficaces lorsque l'agent exerce des fonctions nécessitant l'intégrité de ses capacités, mentales et physiques : conduite d'engin ou de véhicule, manipulations sur des produits dangereux, travaux mécaniques, travaux en hauteur, travaux d'ordre électrique, interventions de toute nature sur navires, etc.

Pour ce faire, l'employeur ou son représentant doit faire en sorte d'écarter l'agent des risques professionnels auxquels il pourrait se trouver exposé dans le cadre de son poste de travail en lui proposant un temps de repos, notamment sur place, dans une salle de repos ou un bureau, ou en le faisant accompagner chez le médecin du travail ou un médecin qui pourra prescrire tout examen médical complémentaire qu'il jugerait utile. Durant cette phase, l'agent pourra demander à être assisté d'un membre du personnel de son choix, disponible au regard des nécessités de service.

Eu égard au respect de l'individu, l'application de cette procédure doit revêtir un caractère de discrétion absolue.

L'employeur ou son représentant pourra demander aux salariés présentant des signes extérieurs d'alcoolisation et occupant un poste à risques ou de sécurité, en particulier ceux énoncés ci-après, de se soumettre à un contrôle d'alcoolémie par alcootest ou éthylotest.

Ces contrôles d'alcoolémie sont réalisés dans le respect de la dignité et de l'intimité de la personne. Le salarié pourra demander à être assisté d'un membre du personnel ou d'un représentant du personnel de son choix disponible et à bénéficier d'une contre-expertise de son état au moyen d'analyses ou d'examens médicaux, chimiques ou biologiques.

Le dépistage précité ayant pour objet de faire cesser une situation à risques pour le salarié lui-même ou pour ses collègues de travail ou des tiers, le recours à l'alcootest ou à l'éthylotest est autorisé pour des salariés occupant un des postes à risques ou de sécurité suivants :

- Travaux en hauteur (dont risque de chute à l'eau)
- Conduite et utilisation de machines dangereuses ou à risques pour les salariés eux-mêmes ou à l'égard de tiers (grues, machines électriques, machines à bois, ponts et autres engins...)
- Conduite de véhicules
- Travaux mécaniques et interventions sur tous types d'engins ou machines dangereuses ou à risques

- Travaux d'ordre électrique
- Interventions de toute nature sur navire (par exemple branchement, débranchement de navires ...)
- Interventions de toute nature sur des chantiers ou des zones d'opérations commerciales.

12. INTERDICTION DE FUMER

Conformément aux dispositions du décret du 15 novembre 2006, l'interdiction de fumer est de portée générale et s'applique dans tous les lieux fermés et couverts qui constituent des lieux de travail, notamment locaux, bureaux, emplacements, véhicules de service, cabines de conduite d'engins de levage et de manutention, salles de machinerie...

Cette interdiction s'applique également sur les installations extérieures lorsqu'une telle interdiction fait l'objet d'une signalisation adaptée.

Il est également interdit de vapoter dans les bâtiments de l'établissement fermés et couverts affectés à un usage collectif.

13. REPAS SUR LES LIEUX DE TRAVAIL

Pour des raisons d'hygiène, les repas ne peuvent être pris que dans les locaux adaptés à cet effet.

14. VESTIAIRES

Le personnel doit tenir les armoires-vestiaires en parfait état de propreté.

Il est interdit d'y conserver des denrées périssables ou matières dangereuses, boissons alcoolisées ou substances illicites.

Pour assurer la sécurité et la salubrité des lieux, il pourra être procédé à l'ouverture et/ou au nettoyage des armoires-vestiaires à l'initiative de l'établissement.

Le salarié est préalablement informé de ces opérations dans les meilleurs délais possibles.

Ces opérations ont lieu en principe en présence du salarié dûment invité sauf cas d'urgence ou de force majeure.

Le salarié qui, en raison d'un empêchement justifié, ne peut assister à l'ouverture pourra se faire remplacer par un membre du personnel de son choix, disponible au regard des nécessités de l'activité.

Les clés des armoires-vestiaires doivent être restituées lorsque le salarié quitte définitivement l'entreprise.

CHAPITRE III

DISCIPLINE GENERALE

15. HORAIRES ET DUREE DU TRAVAIL

Chaque salarié doit se conformer aux horaires de travail en vigueur dans l'entreprise et se trouver à son poste aux heures fixées pour le début et pour la fin du travail, sous réserve des droits reconnus aux représentants du personnel.

Les salariés doivent respecter les modifications d'horaires éventuellement décidées par la direction dans les limites et le respect des dispositions légales, réglementaires et conventionnelles, notamment les protocoles d'accords locaux applicables au sein de l'Etablissement.

Tout salarié doit effectuer les heures supplémentaires qui lui sont demandées dans les limites et le respect des dispositions légales, réglementaires et conventionnelles, sauf cas d'impossibilité personnelle ou familiale, ainsi que les astreintes nécessitées dans le cadre des organisations de travail.

16. PRESENCE AU TRAVAIL

Les sorties pendant les heures de travail doivent être exceptionnelles et faire l'objet d'une autorisation expresse de l'employeur ou son représentant, y compris lorsque le salarié souhaite consulter le médecin du travail.

Tout retard éventuel doit être justifié auprès de l'employeur ou son représentant.

Toute absence, quel qu'en soit le motif, doit être justifiée auprès de l'employeur ou son représentant.

Ces dispositions s'appliquent sous réserve des droits reconnus aux représentants du personnel.

En cas de maladie, d'accident, d'accident du travail ou de rechute accident du travail, le salarié doit prévenir sa hiérarchie de son absence par tout moyen, et transmettre obligatoirement à l'établissement dans les 48 heures, sauf cas exceptionnel dûment justifié, un certificat médical indiquant la durée prévisible de l'absence.

En cas de prolongation d'un arrêt maladie ou accident de travail, tout agent doit en informer sa hiérarchie avant la fin de la période en cours et transmettre le certificat médical dans les délais précisés ci-dessus.

Le défaut de production de certificat médical dans les délais entraîne le non versement du complément de salaire prévu par les dispositions conventionnelles.

En cas d'absence pour maladie professionnelle, d'absence pour congé de maternité, d'absence d'au moins trente jours pour accident du travail, maladie ou accident non professionnel, le salarié devra se soumettre, conformément à la loi, à une visite médicale de reprise.

17. DECLARATION D'ACCIDENTS

Tout accident du travail ou tout autre dommage corporel ou non causé à un tiers doit immédiatement, sauf cas de force majeure, faire l'objet d'une déclaration de l'intéressé ou des témoins auprès du supérieur hiérarchique, conformément à la procédure mise en place en interne.

Les accidents du travail bénins, c'est-à-dire ceux ne nécessitant pas de soins autres que ceux pouvant être prodigués à l'infirmerie peuvent faire l'objet d'une simple consignation sur le registre d'infirmerie.

18. ACCES A L'ENTREPRISE

L'entrée et la sortie du personnel s'effectuent selon les itinéraires et accès prévus à cet effet.

Les salariés n'ont accès aux locaux de l'entreprise que dans le cadre de leurs missions professionnelles durant leurs heures de travail ou dans le cadre de leurs missions de représentation du personnel dans le respect des dispositions du Code du travail.

Il est interdit d'introduire ou de faire introduire dans les locaux de l'Etablissement des personnes étrangères à celui-ci sans nécessité de service, sauf autorisation préalable de la direction, et sous réserve des droits propres aux représentants du personnel.

Chaque salarié reçoit une carte portuaire qui devra être restituée à la Direction des Ressources Humaines lors du départ définitif de l'entreprise. Les salariés sont tenus de déclarer immédiatement la perte, destruction ou le vol de leur carte portuaire auprès du bureau des cartes d'accès.

19. DISCIPLINE AU TRAVAIL

Les salariés sont placés sous l'autorité du chef d'entreprise et de toute personne ayant reçu délégation de ce dernier.

Dans l'exécution de leur travail, les salariés sont tenus de respecter, les directives et les instructions émanant de la direction, ainsi que l'ensemble des prescriptions et consignes notamment en termes de sécurité.

Ils doivent faire preuve de correction dans leur comportement vis-à-vis des collègues de travail, de la hiérarchie, et des personnes extérieures à l'entreprise.

20. OBLIGATION DE LOYAUTE, DE DISCRETION ET DEVOIR DE RESERVE

L'ensemble des documents et matériels détenus par le personnel dans l'exercice de ses fonctions est confidentiel et ne peut être divulgué. Ces documents et matériels doivent être restitués sur simple demande de l'entreprise en cas de modification ou de cessation du contrat de travail pour quelque cause que ce soit.

Le personnel est tenu de faire preuve de la plus grande discrétion vis-à-vis de l'extérieur sur l'ensemble des éléments techniques, financiers ou autres dont il aurait pu avoir connaissance à l'occasion de son travail.

En leur qualité d'agent du GPMM, établissement public de l'Etat, le personnel est tenu à un devoir de réserve qu'il doit respecter tant dans le cadre privé que public.

21. UTILISATION DES LOCAUX

Les locaux de l'entreprise, ainsi que l'ensemble des moyens matériels sont réservés à un usage professionnel. Il est par conséquent interdit d'y effectuer un travail personnel.

Il est interdit de faire circuler sans autorisation de la direction des listes de souscription ou de collecte, à l'exception des collectes réalisées notamment à l'occasion de naissance, mariage, départ à la retraite, ou liées aux cotisations syndicales.

La diffusion des publications et tracts syndicaux doit se faire conformément aux dispositions légales, réglementaires et conventionnelles.

L'affichage n'est autorisé que sur les panneaux réservés à cet effet.

22. UTILISATION DES OUTILS ET MATERIELS DE L'ENTREPRISE

Le matériel et les outils de l'entreprise (téléphone, fax, photocopieuses ...) doivent être utilisés pour les besoins de l'activité professionnelle.

L'utilisation du matériel informatique et du système informatique mis à la disposition du personnel pour les besoins de son activité professionnelle, notamment l'Internet et la messagerie électronique, est réglementée dans le cadre de la Charte de l'Utilisateur annexée au présent règlement intérieur.

L'utilisation des ressources informatiques doit être réalisée dans le respect de la législation en vigueur.

Il est, par exemple, interdit d'utiliser les listes d'adresse globale de la messagerie intranet pour diffuser des informations extérieures ou des messages personnels étrangers à la fonction occupée ou aux missions de l'Etablissement.

Lors de chaque ouverture de session, l'utilisateur accepte d'adopter le comportement professionnel décrit dans la Charte de l'Utilisateur et d'appliquer les bonnes pratiques qui participent à la sécurisation du système d'information du GPMM.

23. VEHICULES DE L'ETABLISSEMENT ET VEHICULES PERSONNELS

Seules les personnes expressément autorisées peuvent utiliser les véhicules de l'entreprise dans le respect des dispositions légales et réglementaires et des procédures et modalités définies en interne.

Chaque conducteur est tenu de respecter le Code de la route, les arrêtés préfectoraux pour la conduite et le stationnement des véhicules et d'assumer les conséquences du non respect de ces dispositions.

Le conducteur doit être titulaire du permis de conduire en cours de validité et approprié au type de véhicule utilisé. Il est tenu de signaler immédiatement à l'employeur ou à son représentant toutes les restrictions de conduite dont il est l'objet qu'elles soient réglementaires ou médicales.

Le stationnement des véhicules dans l'enceinte de l'établissement doit s'effectuer sur les parkings prévus à cet effet.

Les véhicules mis à disposition doivent être utilisés exclusivement dans le cadre de l'exercice des fonctions professionnelles ou de mandats syndicaux.

Excepté le cas où l'exercice des fonctions professionnelles et des mandats syndicaux nécessiterait une utilisation sur un trajet domicile/travail, le véhicule doit rester sur le domaine portuaire après la fin du travail, durant les week-ends, RTT et périodes de congés. Ils ne sauraient être utilisés à des fins personnelles pour ceux qui auraient à les conduire.

Tout incident ou accident, quel qu'il soit, doit donner lieu à l'établissement d'un constat amiable d'accident, dûment complété et signé, et doit parvenir dans les 48 heures à la Direction des Affaires Juridiques et au Département Achats et Moyens Généraux de la Direction Administration et Finances.

24. CIRCULATION SUR LE PORT

La circulation sur le port est soumise aux dispositions du Code de la route et du Règlement particulier de police du port en vigueur, approuvé par arrêté préfectoral.

Les conducteurs doivent circuler avec prudence sur les voies autorisées dans l'enceinte de l'établissement et respecter en général les prescriptions du Code de la Route.

Ils doivent également tenir compte des prescriptions particulières en vigueur sur le Port, concernant notamment la vitesse, la signalisation, les limitations à la circulation et au stationnement annoncées par tout dispositif adéquat (barrières, panneaux, pancartes, marquage au sol ...).

CHAPITRE IV

ECHELLE DES SANCTIONS, DROITS DE LA DEFENSE ET PROTECTION DU LANCEUR D'ALERTE

25. SANCTIONS

Tout manquement à l'une des dispositions du règlement intérieur et plus généralement tout agissement d'un salarié considéré comme fautif, pourra en fonction de la gravité des fautes et/ou de leur répétition faire l'objet de l'une ou l'autre des sanctions suivantes :

- l'avertissement écrit du directeur général, d'un directeur, d'un chef de département ou d'un responsable d'activité,
- le blâme avec inscription au dossier,
- la mise à pied temporaire d'une journée à un mois,
- la rétrogradation de catégorie,
- le licenciement pour faute.

26. DROITS DE LA DEFENSE

Toute procédure disciplinaire envisagée à l'encontre d'un agent est diligentée en respectant les obligations légales.

Aucun fait fautif ne peut être invoqué au-delà d'un délai de deux mois à compter du jour où l'employeur en a eu connaissance, à moins que des poursuites pénales n'aient été exercées dans ce même délai.

Aucune sanction antérieure de plus de trois ans à l'engagement de poursuites disciplinaires ne peut être invoquée à l'appui d'une nouvelle sanction.

Toute sanction ayant une incidence sur la fonction, la carrière, la rémunération et la présence du salarié dans l'entreprise est précédée d'une convocation du salarié à un entretien préalable dans les conditions fixées par le Code du travail.

Cette convocation indiquera l'objet de la convocation et précisera la date, le lieu et l'heure de l'entretien ainsi que la faculté pour le salarié de se faire assister par une personne de son choix appartenant au personnel de l'entreprise.

La sanction ne peut intervenir moins de deux jours ouvrables, ni plus d'un mois après le jour fixé pour l'entretien. Elle est motivée et notifiée au salarié.

Lorsque l'agissement du salarié l'a rendue indispensable, une mise à pied conservatoire pourra être prise immédiatement par le Directeur du Port, et ce dans l'attente de la décision définitive.

27. PROTECTION DU LANCEUR D'ALERTE

Il est rappelé que le lanceur d'alerte, tel que défini par les textes réglementaires, bénéficie du dispositif de protection prévu au chapitre II de la loi 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

CHAPITRE V

ENTREE EN VIGUEUR ET MODIFICATION DU REGLEMENT

28. FORMALITES ET DEPOT

Conformément aux prescriptions des articles L.1321-4 et R.1321-2 du Code du travail, le présent règlement a été :

- soumis pour avis aux membres du Comité Social et Economique,
- communiqué en deux exemplaires à l'inspecteur du travail le 9 décembre 2022 accompagné de l'avis des membres du Comité Social et Economique,
- déposé au secrétariat-greffe du Conseil de Prud'hommes de Marseille le 9 décembre 2022,

Il entrera en vigueur le 10 janvier 2023, soit un mois après les formalités de dépôt et de publicité.

Un exemplaire du présent règlement est remis à chaque salarié.

29. MODIFICATION

Toute modification ultérieure, adjonction ou retrait au présent règlement, sera soumis à la même procédure de consultation, de publicité et de dépôt, conformément aux prescriptions de l'article L.1321-4 du Code du travail.

Fait à Marseille,
Le 07 décembre 2022

Le Directeur Général

- Annexe :
- Charte de l'Utilisateur
 - Code de conduite



Hervé MARTEL

Code de conduite

La loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite loi Sapin II, impose la mise en œuvre d'un Code de conduite définissant et illustrant les différents types de comportement à proscrire comme étant susceptibles de caractériser des faits de corruption ou de trafic d'influence. Ce code de conduite est intégré au présent règlement intérieur.

Le présent Code a été adopté conformément aux obligations légales.

I. OBJET

L'objet du présent Code est de déterminer les valeurs et principes généraux qui sont communs à l'ensemble des salariés du GPMM, et ce notamment dans le domaine de l'anticorruption.

La procédure de signalement des comportements ou situations méconnaissant le Code de conduite est mise à disposition du personnel sur le site intranet de l'Etablissement.

II. CHAMP D'APPLICATION

Le présent Code de conduite s'applique à tous les agents du GPMM sans restriction ni réserve.

Il s'applique sur l'ensemble des sites et dans tous les lieux composant le Grand Port Maritime de Marseille.

Ce Code est remis à chaque nouveau salarié de l'Etablissement et est disponible sur son Intranet.

III. LES REGLES DE CONDUITE

La Direction Générale de l'Etablissement considère que le développement de son activité doit se faire dans le respect de l'intégrité de l'ensemble des parties prenantes. Cette intégrité se traduit par une démarche de sensibilisation de l'ensemble des salariés de l'Etablissement aux valeurs liées à la déontologie, à l'éthique et à la probité.

En ce sens, la Direction Générale de l'Etablissement attend de l'ensemble de ses salariés un comportement exemplaire qui implique, tant le respect des obligations légales et réglementaires qui s'imposent à chacun, que des règles de conduite exposées ci-après.

- **Chaque salarié de l'Etablissement doit respecter et veiller au strict respect, au sein de l'Etablissement, de l'ensemble des dispositions législatives et réglementaires en vigueur.**

En ce sens, nul ne doit sciemment participer à la violation d'une loi, et plus largement de toute réglementation qui s'impose à lui.

En cas de doute sur le risque de concrétisation d'une telle violation, chaque salarié de l'Etablissement devra s'abstenir d'agir et en référer à son supérieur hiérarchique direct.

- **Chaque salarié de l'Etablissement doit veiller à ne pas participer, directement ou indirectement, activement ou passivement à toute forme de corruption.**

La corruption doit être entendue comme :

- le fait d'offrir, de promettre ou de donner directement ou indirectement quelque chose de valeur (monétaire ou autre) en échange d'une incitation à agir ou à ne pas agir de manière inappropriée, illégale ou contraire à l'éthique (corruption active) ;
- le fait de solliciter, de demander, de recevoir ou d'accepter de recevoir directement ou indirectement quelque chose de valeur (monétaire ou autre) en échange d'une incitation à agir ou à ne pas agir de manière inappropriée, illégale ou contraire à l'éthique (corruption passive)

La corruption telle qu'elle est définie dans le présent Code doit être comprise comme incluant notamment les dessous de table, l'extorsion, la concussion, les paiements de facilitation, le trafic d'influence ou encore l'atteinte à l'égalité de traitement des candidats pour l'accession à tout type de contrat.

La Direction Générale de l'Etablissement est particulièrement vigilante quant au fait de garantir l'équité dans les relations avec ses clients, ses fournisseurs et l'ensemble de ses interlocuteurs ce qui implique notamment le respect d'une politique « cadeau » exigeante.

En ce sens, la Direction Générale de l'Etablissement a mis en œuvre une politique « cadeau » dont le contenu est annexé au présent code : Annexe – Politique « cadeau » du Grand Port Maritime de Marseille.

- **Chaque salarié de l'Etablissement doit veiller à ne pas participer, directement ou indirectement, activement ou passivement, à toute prise illégale d'intérêts.**

Tout salarié de l'Etablissement devra exercer ses fonctions de manière impartiale et objective. En ce sens, chaque salarié de l'Etablissement doit mettre en œuvre l'ensemble des diligences nécessaires afin d'éviter une situation dans laquelle ses intérêts personnels pourraient interférer avec les intérêts de l'Etablissement. Les conflits d'intérêts personnels surviennent lorsque :

- les intérêts personnels d'un salarié de l'Etablissement sont susceptibles d'entrer directement ou indirectement en conflit avec les intérêts de l'Etablissement interférant ainsi avec le strict respect, par le salarié de l'Etablissement, de ses responsabilités professionnelles ;
- un salarié de l'Etablissement est susceptible de posséder, directement ou indirectement des intérêts qui pourraient influencer ou seulement paraître influencer sur la manière dont il s'acquitte de ses fonctions et prend ses décisions.

En conséquence, un salarié de l'Etablissement qui serait susceptible de se trouver dans une situation de conflit d'intérêts devra directement en informer son supérieur hiérarchique, et le cas échéant se retirer, afin d'éviter de prendre, de participer ou simplement d'être présent lorsqu'une décision dans laquelle il est susceptible d'avoir directement ou indirectement un intérêt, sera prise.

Ce devoir de retrait vaut, dans les mêmes conditions, dès l'engagement des discussions préparatoires à une prise de décision qui engagera l'Etablissement.

Dans un souci d'efficacité et afin d'éviter tout soupçon de partialité dans la prise de décision, chaque salarié de l'Etablissement a la possibilité, lorsqu'il en a la capacité, de faire un inventaire des situations dans lesquelles il serait susceptible d'être dans une situation pouvant créer un conflit d'intérêts ; un échange avec le supérieur hiérarchique

pourra permettre d'élaborer le cas échéant une solution destinée à prévenir ce risque en amont.

- **Chaque salarié de l'Etablissement doit veiller à traiter de manière appropriée l'ensemble des informations et des connaissances mises à sa disposition.**

Les informations et les connaissances de l'Etablissement constituent une de ses principales richesses et doivent donc faire l'objet d'une protection et d'un traitement particulier.

En ce sens, l'Etablissement ne tolérera pas qu'un de ses salariés transmette ou communique sciemment à l'intérieur ou à l'extérieur de l'Etablissement une information qui serait notamment :

- inexacte ou incorrecte et alors susceptible d'induire en erreur son destinataire ;
- une information confidentielle ;
- une information de nature à entraîner une rupture d'égalité dans le traitement des candidats et candidats potentiels à l'accession à un contrat.

Les salariés de l'Etablissement ayant accès, dans le cadre de leurs activités professionnelles, à des informations confidentielles concernant l'Etablissement, sa stratégie, ses projets, sa politique ou encore ses biens, doivent protéger et s'abstenir d'utiliser indûment ces informations afin qu'elles ne soient pas utilisées de manière inappropriée ou au bénéfice d'un tiers.

IV. FORMATION

L'ensemble de ce dispositif a vocation à être précisé au regard des risques inhérents à chaque emploi dans les domaines de la corruption.

Pour cela, l'Etablissement déploie et maintient un programme de formation ciblé sur les vulnérabilités inhérentes à chaque emploi. Les modules de formation permettront à chaque salarié de l'Etablissement d'identifier les risques et d'appréhender au mieux les comportements à adopter dans des situations mettant en jeu les principes liés à la déontologie, à l'éthique et à la probité.

Le niveau des formations dispensées sera adapté et proportionné au niveau de vulnérabilité inhérent à chaque emploi.

V. ACCEPTATION ET RESPECT DU CODE

Chaque salarié de l'Etablissement est tenu de respecter l'ensemble des dispositions du présent Code.

Compte-tenu des évolutions de son activité et des risques liés à celle-ci, et ce notamment en matière de corruption, l'Etablissement examinera régulièrement la nécessité d'actualiser le présent Code afin que celui-ci soit constamment en cohérence avec la cartographie des risques de l'Etablissement.

L'Etablissement communiquera et diffusera la version du Code alors en vigueur.

Le présent Code étant annexé au règlement intérieur de l'Etablissement, chaque salarié de l'Etablissement est réputé en avoir pris connaissance et accepté le contenu.

VI. ECHELLE DES SANCTIONS, DROITS DE LA DEFENSE ET PROTECTION DU LANCEUR D'ALERTE

1. Sanctions

Tout manquement à l'une des dispositions du présent Code de conduite pourra, en fonction de la gravité des fautes et/ou de leur répétition, faire l'objet de l'une ou l'autre des sanctions suivantes :

- l'avertissement écrit du directeur général, d'un directeur, d'un chef de département ou d'un responsable d'activité,
- le blâme avec inscription au dossier,
- la mise à pied temporaire d'une journée à un mois,
- la rétrogradation de catégorie,
- le licenciement pour faute.

2. Droits de la défense

Toute procédure disciplinaire envisagée à l'encontre d'un agent est diligentée en respectant les obligations légales.

Aucun fait fautif ne peut être invoqué au-delà d'un délai de deux mois à compter du jour où l'employeur en a eu connaissance, à moins que des poursuites pénales n'aient été exercées dans ce même délai.

Aucune sanction antérieure de plus de trois ans à l'engagement de poursuites disciplinaires ne peut être invoquée à l'appui d'une nouvelle sanction.

Toute sanction ayant une incidence sur la fonction, la carrière, la rémunération et la présence du salarié dans l'entreprise est précédée d'une convocation du salarié à un entretien préalable dans les conditions fixées par le Code du travail.

Cette convocation indiquera l'objet de la convocation et précisera la date, le lieu et l'heure de l'entretien ainsi que la faculté pour le salarié de se faire assister par une personne de son choix appartenant au personnel de l'entreprise.

La sanction ne peut intervenir moins de deux jours ouvrables, ni plus d'un mois après le jour fixé pour l'entretien. Elle est motivée et notifiée au salarié.

Lorsque l'agissement du salarié l'a rendue indispensable, une mise à pied conservatoire pourra être prise immédiatement par le Directeur du Port, et ce dans l'attente de la décision définitive.

3. Protection du lanceur d'alerte

Il est rappelé que le lanceur d'alerte, tel que défini par les textes réglementaires, bénéficie du dispositif de protection prévu au chapitre II de la loi 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Annexe au Code de conduite - Politique « cadeau »

La présente politique « cadeau » envisage tant les situations où l'Etablissement serait l'offrant que celle où il serait destinataire du cadeau.

Par cadeau, il est entendu tout avantage, de quelque nature que ce soit, octroyé sans contrepartie soit :

- par un tiers au profit d'un salarié de l'Etablissement,
- par un salarié de l'Etablissement au profit d'un tiers.

Lorsque l'Etablissement entretient des relations commerciales, institutionnelles ou d'affaires avec un tiers, le salarié de l'Etablissement doit respecter scrupuleusement les règles et les principes directeurs de la politique « cadeau » de l'Etablissement avant d'accepter de recevoir ou d'offrir un cadeau.

Ces règles et principes directeurs sont exposés ci-après.

1. Interdiction d'accepter les cadeaux proposés si une période de négociation et/ou de sélection est engagée dès lors qu'il existe un lien, même potentiel, de candidat/adjudicateur entre l'offrant et le destinataire.

Cette interdiction vaut même lorsque l'offrant et le destinataire entretiennent déjà une relation commerciale, institutionnelle ou d'affaires.

4. Interdiction des cadeaux dont la valeur dépasse le seuil déterminé

Aucun salarié de l'Etablissement ne pourra accepter ou offrir un cadeau dont la valeur unitaire excède le montant fixé par le Code général des impôts. A titre d'information ce montant, qui est susceptible d'évoluer, s'élève à 69 euros TTC¹ en 2020.

5. Interdiction de certains cadeaux

Dans tous les cas, les cadeaux suivants sont interdits :

- les dons en espèces ou équivalents, les prêts, les titres de placement ;
- les paiements faits à des personnes qui, en raison de leurs fonctions, disposent du pouvoir de sécuriser ou d'accélérer l'exécution de démarches ou de formalités qui incombent à l'Etablissement ;
- les cadeaux sous-conditions ou sollicités ;
- les cadeaux reçus ou envoyés au domicile d'un salarié ;
- les cadeaux non conformes aux lois et aux réglementations applicables ;
- les produits et services à caractère illégal ou contraires à la dignité de la personne ;
- les prestations de l'offrant à titre gratuit ou proposées à une valeur inférieure aux prix du marché.

¹ Article 28-00 A du Code général des impôts

6. Principe de prudence

Le cadeau doit être en lien avec la promotion du savoir-faire, le développement de l'activité commerciale du destinataire ou être en lien avec la qualité des relations de travail qui existent entre l'offrant et le destinataire.

Le cadeau ne doit en aucun cas pouvoir porter atteinte à la neutralité du processus de décision du destinataire ou engendrer une suspicion de corruption.

Le nombre, la fréquence et la valeur des cadeaux demeurent raisonnables.

7. Principe de transparence

Tout salarié de l'Etablissement qui sera sollicité et/ou acceptera et/ou offrira un cadeau devra directement en informer son supérieur hiérarchique direct.

Chaque supérieur hiérarchique dressera une liste des cadeaux reçus et/ou offerts par les salariés de l'Etablissement exerçant leurs fonctions sous sa direction.

Chaque directeur communiquera semestriellement au Comité d'Ethique (cf procédure de signalement) la liste des cadeaux perçus et/ou offerts par les personnels dont il a la responsabilité.

8. Cas particuliers

Lorsque la réception ou l'offre d'un cadeau fait partie intégrante de règles de savoir vivre, de la culture, de coutumes applicables et sous réserve de la validation a posteriori du Comité d'Ethique, il pourra être dérogé à l'interdiction figurant à l'article 2. de la présente politique « cadeau ».

Lorsque le salarié de l'Etablissement offre le cadeau, il ne pourra être dérogé à l'article 2. qu'après validation, a priori, du Comité d'Ethique.

Lorsque le salarié de l'Etablissement est destinataire du cadeau, il ne pourra être dérogé à l'article 2. qu'après validation, a posteriori et dans les meilleurs délais, du Comité d'Ethique.

Dans l'hypothèse où la dérogation ne serait pas validée par le Comité d'Ethique, celui-ci se prononcera également sur le devenir du cadeau.

Toute contravention à la décision rendue par le Comité d'Ethique sera considérée comme une violation du Code de conduite anticorruption de l'Etablissement.

9. Sanctions

La présente politique « cadeau » est annexée au Code de conduite, lui-même annexé au règlement intérieur. Par conséquent, la méconnaissance des règles édictées constitue une violation du Code de conduite et pourra faire l'objet d'une sanction dans les conditions définies par son article VI. « *Echelle des sanctions et droits de la défense* ».



DPO
Data Protection Officer

Marseille Fos
Le port euroméditerranéen



Charte Utilisateur

Système d'Information du Grand Port Maritime de Marseille

ENTREE EN VIGUEUR DE LA CHARTE :

La présente charte a été présentée au CHSCT du GPMM lors de la séance ordinaire du 15 octobre 2015.

La présente charte a été présentée devant le comité d'entreprise lors de la séance du 29 octobre 2015.

La présente charte a été approuvée le 15 décembre 2015.

Changement du logo CIL par le logo DPO le 25 mai 2018



La reproduction de tout ou partie de ce document est subordonnée à l'autorisation explicite du
Grand Port Maritime de Marseille

Version 15 octobre 2015 modifiée le 25 mai 2018





Préambule

Le Grand Port Maritime de Marseille (GPMM) met en œuvre un système d'information et de communication nécessaire à l'exercice *de ses missions*. Il met ainsi à disposition de ses collaborateurs des outils informatiques, et de communication d'entreprise.

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication du GPMM. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle du GPMM.

Cette Charte qui fait partie intégrante du règlement intérieur, a pour objet de préciser les droits et devoirs puis la responsabilité des utilisateurs en accord avec les textes législatifs et réglementaires afin d'instaurer un usage correct des ressources informatiques et des services réseaux (intranet & internet).

L'utilisation de tout système informatique relié à un réseau suppose de la part des utilisateurs le respect d'un certain nombre de règles issues de la **Politique de Sécurité des Système d'Information du GPMM**, dont le rôle est d'assurer la sécurité et les performances des traitements, la préservation des données confidentielles, et le respect des législations applicables.

A fortiori, le raccordement à un réseau public tel qu'Internet rend le respect des dites règles encore plus impératif.

La présente charte est régie par les lois françaises indépendamment de tout conflit de dispositions légales.

Dans l'hypothèse où l'une quelconque des dispositions ci-après serait tenue pour nulle, illégale ou non valide en vertu de tout règlement ou loi présent ou futur, ladite disposition serait réputée non écrite.

L'ensemble du présent document restera en vigueur dans toute la mesure juridiquement possible, à l'exception de la clause réputée non écrite.

Les titres de la présente charte ne servent que de référence et ne peuvent limiter ni affecter de quelque manière que ce soit ses termes ou dispositions.





Article 1 - Champ d'application

Les règles et obligations définies dans cette charte s'appliquent à tout utilisateur* du Système d'Information de l'établissement (GPMM) pendant la durée de ses activités professionnelles au sein de celui-ci.

Tout utilisateur est responsable de l'usage qu'il fait des outils et ressources informatiques et de communication mis à sa disposition par le GPMM. Leur utilisation à titre privé est tolérée, mais doit être raisonnable et ne doit pas perturber le bon fonctionnement du service.

La charte est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur l'intranet du GPMM dans les ressources documentaires sur le dossier \AQSSI-DPO\Chartes & plan de sécurité. Elle est systématiquement remise à tout nouvel arrivant qui reconnaît, en signant l'attestation ci-après annexée, en avoir pris connaissance et en avoir compris les termes.

Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées. Le DPO se tient à la disposition de tout utilisateur qui souhaite des explications complémentaires.

[*] Voir la définition dans le glossaire.



Article 2 - Conditions d'accès (sur un poste utilisateur)

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies ci-dessous :

Le droit d'accès à une partie du système d'information est soumis à l'autorisation de son responsable-détenteur*. Ce droit est limité exclusivement à des activités qui sont rendues nécessaires par l'exercice des missions confiées à l'utilisateur et dans le respect de la législation et de la réglementation en vigueur. L'utilisation à des fins non professionnelles est tolérée dans les limites définies à l'article 5.

Le droit d'accès est formalisé par un compte nominatif applicatif personnel non transmissible et incessible, même temporairement, et révocable dans le cas d'un usage contraire aux exigences de la présente charte ou d'une suspicion de compromission.

En particulier, l'accès aux ressources informatiques repose strictement sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son arrivée au GPMM. Un mot de passe est associé à cet identifiant de connexion. Les moyens d'authentification sont personnels et confidentiels. Le mot de passe doit être composé de 8 caractères minimum combinant chiffres, lettres minuscules, lettres majuscules et caractères spéciaux. Il ne doit comporter ni le nom, ni le prénom composant l'identifiant d'ouverture de la session de travail et doit être différent des 3 précédents mots de passe. Il doit être renouvelé tous les 6 mois. Ces caractéristiques sont contrôlées par le système et peuvent se durcir en fonction de l'évolution des menaces auxquelles le GPMM est confronté.

L'utilisateur est informé que l'attribution d'un compte nominatif constitue une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette attribution ne confère pas aux moyens d'information mis à sa disposition un caractère personnel.

L'utilisateur est tenu de veiller à la protection et la confidentialité des différents moyens personnels d'authentification et des moyens d'accès qui sont mis à sa disposition. Le corollaire étant qu'il est interdit d'utiliser les codes d'accès (nom d'utilisateur, mot de passe) et moyens d'accès d'un autre utilisateur.

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



L'utilisateur ne doit pas notamment :

- * Accéder ou tenter d'accéder à des documents dont l'accès est restreint ou limité, ou pour lesquels il n'a pas d'autorisation d'accès, collecter des informations sur un autre utilisateur, usurper son identité, tenter de décrypter ou de découvrir les mots de passe d'un autre utilisateur, intercepter ou interrompre ses communications.
- * Percer ou contourner les mécanismes de protection de fichiers, banques de données, ordinateurs, systèmes ou réseaux informatiques.
- * Essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur.
- * Utiliser le même mot de passe d'accès au réseau GPMM, pour un usage personnel (Accès à un réseau social, messagerie personnelle ...).

Article 3 – Règles générales d'utilisation, de sécurité et de bon usage

L'utilisateur doit utiliser les moyens mis à sa disposition dans le respect de la législation et de la réglementation en vigueur. Il doit notamment s'abstenir de tout comportement illicite, ou constitutif d'un piratage ou d'une fraude relative aux systèmes d'information.

Tout utilisateur est responsable des moyens qui lui sont confiés ou fournis, de l'usage qu'il en fait et des informations qu'il possède. Il s'engage à ne pas effectuer des opérations pouvant nuire au fonctionnement du réseau, à l'intégrité de l'outil informatique, et aux relations internes et externes de l'établissement.

L'utilisation des moyens doit être rationnelle et loyale afin d'éviter leur saturation et leur utilisation à des fins qui ne sont pas professionnelles.

La sécurité de l'Information au sein du GPMM repose entre autres sur l'exemplarité du comportement des utilisateurs, le respect des règles élémentaires d'hygiène informatique (rappelé lors de chaque ouverture de session Windows) et en premier lieu, par le respect de la présente Charte Utilisateur et le non-contournement de la politique de sécurité (PSSI).

Tout utilisateur s'engage, notamment, à respecter les règles de sécurité suivantes:

A – Sur son poste de travail

- * Il doit signaler, dans les plus brefs délais, en cas de doute sur un évènement informatique suspect, à son supérieur hiérarchique ou à la hotline, toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement et toute alerte virale sur son poste de travail.
- * Il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde mis à sa disposition. Il est responsable des droits qu'il donne aux autres utilisateurs.
- * Il ne doit pas masquer sa véritable identité, emprunter ou chercher à emprunter l'identité d'un autre utilisateur ou d'un tiers.
- * Il ne doit pas modifier les paramétrages du poste de travail ainsi que sa configuration physique ou logicielle.



- * Il ne doit pas installer de logiciels sans l'autorisation du Département du Système d'Information (DSI).
- * Il ne doit pas connecter d'ordinateurs personnels au réseau de l'entreprise. Seuls les supports amovibles (CD-ROM, clé USB, disque dur externe, ...) fournis par le GPMM peuvent être connectés sur les postes de travail, sans autorisation. Les supports amovibles personnels (CD-ROM, clé USB, disque dur externe, ...) doivent au préalable faire l'objet d'une demande de validation auprès de DSI.
- * Il ne doit pas déplacer son poste de travail (sauf s'il s'agit d'un «équipement nomade», dans les conditions prévues au paragraphe B ci-dessous).
- * Il ne doit pas copier, modifier, désinstaller les logiciels propriétés du GPMM.
- * Il doit verrouiller son ordinateur dès qu'il quitte son poste de travail pour ne pas laisser des ressources ou applications accessibles et éteindre son poste le soir, avant de partir, afin de rendre effectives les mises-à-jour des correctifs de sécurité.
- * Il doit s'assurer que les informations confidentielles en sa possession ne peuvent être accessibles par des utilisateurs non autorisés. Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique.
- * Il ne doit accéder, modifier ou supprimer que les seules données dont la garde lui est confiée, de plein droit ou par délégation, et sur lesquelles il a été dûment autorisé à effectuer ces opérations.
- * Il s'engage à ne pas mettre à la disposition d'utilisateurs internes ou externes non autorisés un accès aux informations ou aux réseaux, à travers des équipements dont il a l'usage.
- * Il ne doit utiliser que les moyens de cryptologie en usage dans l'Etablissement, et respecter la réglementation en vigueur en la matière.
- * Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des moyens informatiques auxquels il accède, notamment par l'insertion et la propagation de virus, logiciels malveillants ou parasites, la destruction ou la modification de données ou de logiciels.
- * Il ne doit pas utiliser les serveurs à des fins illicites ou frauduleuses ou pour afficher un contenu illégal, agressif, abusif, préjudiciable, portant atteinte à la vie privée ou pouvant choquer de quelque manière que ce soit.
- * Il ne doit pas utiliser l'outil informatique à des fins de harcèlement, menace, diffamation dénigrement ou tout acte réprimé par le droit en vigueur.

En outre, il convient de rappeler que les visiteurs (y compris les intervenants des sociétés prestataires ayant conclu un contrat de marché public avec le GPMM) ne peuvent et sous condition, avoir accès au Système d'Information du GPMM sans l'accord formel et préalable du DSI. Les représentants légaux ou juridiquement habilités des personnes morales ayant accès, pour quelle que raison que ce soit au SI du GPMM doivent s'engager à faire respecter la présente charte par leurs propres salariés. Dès lors, les contrats signés entre le GPMM et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation ainsi qu'une clause par laquelle le cocontractant déclare avoir pris connaissance de la présente charte.

B - Equipements nomades d'entreprise

On entend par «**équipements nomades d'entreprise**» tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, etc.. ..).

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, notamment par chiffrement. Cette sécurisation particulière doit être demandée au DSI, par le responsable-détenteur des données que ces équipements peuvent stocker.

Quand un ordinateur portable a été doté d'un antivol, cet antivol doit être utilisé dans le bureau de l'utilisateur qui en a l'usage afin que cet ordinateur soit physiquement attaché (sauf quand l'utilisateur est physiquement présent dans son bureau).

L'utilisation de Smartphones (ou tablettes) personnels, reliés à l'Internet pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Afin de réduire ces risques, ces équipements sont sécurisés par le DSI en y incluant le verrouillage automatique.

C - Procédures spécifiques aux matériels de prêt

L'utilisateur doit renseigner et signer un registre, tenu par le Département du Système d'Information, actant la remise de l'équipement nomade vu au point précédent. L'utilisateur en assure la garde et la responsabilité et doit informer le DSI en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte.

L'utilisateur est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements.

Lors de son départ, l'utilisateur doit restituer au DSI les matériels mis à sa disposition. Le retour des matériels est consigné dans le registre.

Article 4 - Contrôle, imputabilité et traçabilité des actions

Le GPMM a un total accès aux fichiers professionnels. Cet article décrit les modalités d'intervention du Département du Système d'Information (DSI).

Le DSI assure le bon fonctionnement et la sécurité des réseaux informatiques, des moyens informatiques et de communication du GPMM. Les personnels de ce service disposent d'outils techniques leur permettant de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place dans le seul but d'en assurer la sécurisation et l'intégrité.

Dans le cadre de leurs fonctions, les agents du DSI pourront avoir accès à l'ensemble des données techniques d'entreprise. Ces agents sont assujettis au devoir de réserve, à ce titre ils s'engagent à respecter les règles applicables aux contenus des documents qu'ils seraient amenés à examiner et à en préserver la confidentialité. A cet effet, les agents du DSI signent un document d'habilitation spécifique appelé « Engagement de confidentialité pour les informaticiens », annexé au présent document, contenant les exigences et les devoirs auxquels ils sont soumis.

L'utilisateur est expressément informé que le GPMM se réserve le droit de surveiller, contrôler et d'opérer des traces à tout moment de l'utilisation faite du Système d'Information. En cas d'anomalies, incidents ou d'usage non conformes aux besoins professionnels, des recherches pourront être mises en œuvre afin d'en trouver l'origine, notamment pour répondre aux requêtes émises par les autorités publiques compétentes (tribunaux, police). A ces fins, elle met en œuvre des moyens d'enregistrement et d'analyse. Les informations associées jouissent d'une protection particulière contre tout risque de divulgation. Par ailleurs et dans le respect des dispositions législatives et réglementaires, notamment par référence à la Loi «informatique et libertés», le GPMM met en œuvre des moyens de contrôle et d'investigation utiles à la sauvegarde de ses intérêts. Ces contrôles sont limités aux mesures quantitatives en ce qui concerne les informations à caractère «privé». Lorsque les circonstances l'exigent, le GPMM peut être amenée à restreindre, voire fermer, sans préavis tout accès avec l'extérieur.



Dans le strict respect des textes législatifs et réglementaires en vigueur et afin de surveiller le fonctionnement et de garantir la sécurité du système d'information du GPMM, différents dispositifs sont mis en place :

A - Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant d'assurer par une meilleure gestion, la sécurité des flux et la confidentialité des données, sont mis en œuvre. Il s'agit notamment du filtrage ou de l'interdiction d'accès à certains sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, messagerie instantanée, échanges de données de fort volume...) et de la possible analyse des flux HTTPS à fin d'identification de logiciels malveillants ou de détection de flux sortants ou entrants apparaissant anormaux.

B - Les systèmes automatiques de traçabilité

L'objectif du GPMM est d'assurer la sécurité des systèmes d'informations et de garantir une utilisation normale de ces systèmes, non de réaliser un contrôle individuel de l'activité des agents.

Le DSI opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Il s'appuie, en particulier sur des fichiers automatiques de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : comptes, dates, activités logicielles, postes de travail et objet de l'évènement. Aucune information sur les contenus n'est tracée.

Le DSI est le seul utilisateur de ces fichiers de journalisation qui sont effacés à l'expiration d'un délai de 6 mois, sauf réquisitions judiciaires.

C - La surveillance du poste de travail

A des fins de maintenance correctrice, curative ou évolutive, le DSI peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le DSI peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

Article 5 - Utilisation des moyens informatiques à des fins privées

Il est rappelé que les moyens mis à disposition de l'utilisateur doivent être utilisés à des fins professionnelles, dans le cadre des missions qui lui sont confiées.

Leur utilisation résiduelle à titre privé est néanmoins tolérée, dans les conditions décrites au présent article.

L'utilisation des SI du GPMM à des fins privées ne doit pas revêtir de caractère abusif (ni dans sa fréquence ni dans sa durée), excessif, incompatible avec l'activité professionnelle exercée, illicite ou frauduleux et doit respecter la législation et la réglementation en vigueur.

Notamment, la détention, la diffusion ou l'exportation d'images à caractère pédophile, ou la diffusion de contenus à caractère raciste ou antisémite est interdite. La responsabilité du GPMM ne peut être engagée quant à la conservation et l'utilisation de cet espace.

Toute utilisation du système d'information du GPMM (toute information, toute connexion, tout message électronique, tout fichier créé par l'utilisateur, toute communication téléphonique ou SMS, etc.) est présumée avoir un caractère professionnel, à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée (qu'elles figurent sur son poste de travail, sa messagerie ou toute autre ressource), qui ne pourront être ouvertes hors la présence de l'utilisateur.

Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet.

Un dossier nommé « PERSONNEL_Prénom-NOM-DE-FAMILLE » (par exemple C:\PERSONNEL_Jean-DUPONT) pourra ainsi être constitué sur le poste de travail en dehors du dossier professionnel intitulé « Mes Documents ». En effet, le simple classement d'un fichier dans le dossier « Mes Documents » figurant sur le poste de travail de chaque utilisateur ne suffit pas à lui donner un caractère privé.



Seul le contenu de ce dossier privé sera soumis au secret des correspondances et doit notamment contenir les fichiers d'archivage des courriels à caractère personnel. La sauvegarde de ce dossier incombe à l'utilisateur qui en est le seul responsable. Tous les fichiers situés en dehors de ce dossier auront un caractère professionnel.

En cas de maintenance ou en cas de panne du poste de travail, le rétablissement des données personnelles sera effectué dans la mesure du possible mais sans aucune obligation de réussite de la part du GPMM.

En cas de lenteur ou problème technique sur le poste de travail en raison d'un espace disque saturé par le dépôt de documents personnels, le DSI se réserve le droit de demander l'effacement des données personnelles.



Article 6 - Respect des droits de propriété intellectuelle

Le GPMM rappelle que l'utilisation du système d'information implique par tout utilisateur le respect de ses droits de propriété intellectuelle ainsi que ceux de ses cocontractants ou de tout tiers détenant de tels droits.

Toute utilisation du système d'information à des fins de reproduction, de représentation de mise à disposition ou de communication au public d'œuvres protégées par un droit d'auteur ou un droit voisin sans autorisation de la personne détentrice de ce droit est notamment interdite et peut être sanctionnée par les autorités judiciaires compétentes.

Tout comportement non-conforme au code de la propriété intellectuelle à partir d'un poste de travail sera imputé à son utilisateur habituel, à moins qu'il n'apporte la preuve qu'il n'est pas responsable de ce comportement.

L'usage d'un logiciel suppose, en général, la détention d'une licence. Les éventuelles copies de logiciels doivent être strictement conformes aux engagements pris par le GPMM dans le contrat de licence.

Chaque utilisateur doit donc respecter le droit en vigueur relatif au droit de propriété intellectuelle et droits voisins, et notamment les dispositions ci-dessous :

- * Il est strictement interdit d'effectuer des copies de logiciels pour quelque usage que ce soit, seule une copie de sauvegarde pourra être effectuée par le seul personnel habilité à cette fin.
- * L'utilisateur doit utiliser tout logiciel dans les conditions de licence souscrite et ne doit pas contourner les restrictions d'utilisation d'un logiciel.
- * Il est interdit d'installer un logiciel commercial sans licence.
- * L'utilisateur ne doit pas violer les droits d'un tiers y compris les droits d'auteur, marques de commerce, brevets, secrets commerciaux et autres propres à la propriété intellectuelle.
- * Il est interdit de communiquer - intégralement ou partiellement - une œuvre ou sa reproduction au public sans autorisation préalable du ou des auteurs. Les logiciels, les bases de données et autres créations telles que les articles, photographies, pages WEB, fichiers musicaux ou vidéos, etc. constituent notamment des œuvres au sens du code de la propriété intellectuelle.

- * Il est également interdit, même lorsque l'œuvre a été divulguée par son auteur, d'en effectuer des copies ou reproductions (en dehors du droit à la copie privée ou de sauvegarde qui implique l'obligation de détention d'un exemplaire de l'œuvre acquis légalement, ou dans le cadre de l'utilisation de logiciels libres), ou de les modifier. Cette interdiction peut être levée par l'autorisation de l'auteur ou/et de l'éditeur/producteur.
- * Le téléchargement illégal, soit le fait d'acquérir ou d'accéder via internet à des œuvres protégées par des droits d'auteurs, sans que soient rémunérés les ayants droit est interdit.
- * Il est rappelé aux utilisateurs que le téléchargement illégal d'une œuvre protégée par les droits d'auteur expose son auteur à des risques de sanction pénale et que tout téléchargement à partir d'un poste de travail sera imputé à son utilisateur habituel. L'utilisation des logiciels (source ou binaire) et plus généralement de tout document (fichier, image, son, etc.) faite de manière non conforme au code de la propriété intellectuelle est susceptible de constituer un délit de contrefaçon, lequel est sanctionné pénalement dans les conditions prévues aux articles L335-1 et suivants du code de la propriété intellectuelle.

L'article L. 131-2 du code du patrimoine prévoit que «Les logiciels et les bases de données sont soumis à l'obligation de dépôt légal dès lors qu'ils sont mis à disposition d'un public par la diffusion d'un support matériel, quelle que soit la nature de ce support.». Les produits réalisés au sein d'un service et mis à la disposition du public sont donc soumis à l'obligation du dépôt légal. Cette formalité doit être respectée sous peine de sanctions pénales.

Article 7 - Protection des données à caractère personnel (DCP)

Le règlement (UE) 2016/679 du parlement européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel définit les conditions dans lesquelles ces traitements peuvent être effectués.

Le GPMM a désigné, le 25 mai 2018, un délégué à la protection des données à caractère personnel appelé DPO pour Délégué à la Protection des Données (ex Correspondant Informatique et Libertés).

Le DPO recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel du GPMM au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande. Elle est également diffusée sur l'intranet du GPMM.

Le DPO est obligatoirement consulté par le responsable des traitements lors de la création de tout fichier contenant des informations à caractère personnel et les demandes de traitement y afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers, afin de procéder aux formalités préalables à la mise en œuvre. Toute personne sur laquelle des informations figurent dans un tel fichier doit être informée de l'existence de ce fichier, de sa finalité, de l'existence d'un droit d'accès, de rectification, le cas échéant d'opposition, relatif aux données qui le concerne ainsi que des modalités de mise en œuvre de celui-ci, et ce dès la collecte des informations la concernant. En cas de difficultés rencontrées lors de l'exercice de ce droit, les personnes concernées peuvent saisir le DPO du GPMM : dpo@marseille-port.fr.

La constitution, le recueil, l'utilisation, le traitement, la transmission de tout ou partie de fichiers comportant des informations nominatives ne peuvent intervenir que dans le strict respect des dispositions légales en vigueur. Si au cours de son activité, l'utilisateur est amené à réaliser une ou plusieurs opérations ci-avant précitées, il doit auparavant obtenir l'autorisation du responsable-détenteur de ces données. Celui-ci consulte par écrit le DPO et doit se conformer à l'avis qui lui sera remis.

Tout utilisateur ayant accès à des fichiers contenant des données à caractère personnel, doit signer un document d'habilitation spécifique appelé « Engagement de confidentialité DCP », annexé au présent document, contenant les exigences et les devoirs auxquels il est soumis et qu'il s'engage à respecter. Tous les utilisateurs des logiciels HRAccess, GESPASS et CAPORT sont notamment concernés.





Article 8 – Gestion des absences et des départs

En cas de départ ou d'absence prolongée prévue, chaque utilisateur prend, dans la mesure du possible et si nécessaire, les précautions propres à ce que la poursuite de l'activité continue d'être assurée. Pour cela, il doit :

- privilégier le dépôt des fichiers de travail sur l'espace partagé, sur un serveur du GPMM par les membres de son activité ou de son équipe,
- informer sa hiérarchie des modalités d'accès aux ressources mises à sa disposition, étant ici rappelé que les données non situées dans un espace identifié comme privé, sont présumées être professionnelles,
- informer ses interlocuteurs de son absence, en utilisant les fonctions de notification d'absence de la messagerie électronique.

En cas d'absence prolongée et imprévue et afin de garantir la continuité de service, le GPMM peut avoir la nécessité d'accéder à la messagerie électronique d'un agent, sous les conditions suivantes :

- l'agent est injoignable ou dans l'incapacité de transférer ses messages,
- la décision est prise par le directeur de l'agent,
- la manipulation est effectuée par le DPO avec les indications de recherches précises fournies par le responsable hiérarchique de l'agent,
- l'agent est immédiatement informé de la manipulation sur sa messagerie.

Seuls sont transférés, les messages présentant un intérêt, provenant d'un expéditeur extérieur au GPMM et pour lesquels aucun autre destinataire GPMM n'est connu. Le gestionnaire d'absence est actionné pour indiquer aux correspondants vers qui rediriger leurs mails.

Lors de son départ du GPMM, l'utilisateur est tenu de remettre au DSI, l'ensemble des moyens informatiques et de communication mis à sa disposition pour l'exercice de son activité professionnelle. L'utilisateur est averti que le lendemain de son départ, son compte d'accès à son poste de travail est désactivé, que sa boîte mail est désactivée et que dans un délai maximum d'un mois après son départ, ses comptes sont supprimés.

L'utilisateur, responsable de la destruction de ses données privées doit donc supprimer ses fichiers et documents personnels AVANT son départ.

Toute copie de documents professionnels doit être préalablement autorisée par le supérieur hiérarchique.

C'est avant le départ de l'agent, que son supérieur hiérarchique doit se préoccuper de la récupération des éventuelles données professionnelles que l'agent est le seul à détenir. Ceci afin de pouvoir évaluer la pertinence de ce qui doit être récupéré et de ce qui peut être détruit.



Article 9 – Règles particulières relatives à l’usage des services Internet, messagerie, forum, téléphonie

Il est rappelé aux utilisateurs que l’usage d’Internet, de la messagerie électronique et des moyens de téléphonie est soumis à l’ensemble des règles de droit en vigueur, à celles de la présente charte et aux dispositions particulières du présent article.

D’une manière générale, il est interdit de détourner l’outil d’information et la connexion internet de l’usage pour lequel il a été mis à disposition.

A - Internet

L’utilisateur doit faire usage des services Internet/intranet dans le cadre exclusif de ses activités professionnelles, des missions de l’établissement et dans le respect du droit en vigueur. Aucune publication d’information à caractère privé sur les ressources du SI de l’établissement n’est admise, sauf dérogation admise par le responsable-détenteur de la ressource (par exemple les pages mariages et naissances du site Intranet).

Si une utilisation ponctuelle et raisonnable (au sens de la jurisprudence) pour un motif personnel, des sites internet dont le contenu n’est pas contraire à la loi, à l’ordre public, n’est pas incompatible avec l’activité professionnelle exercée et ne met pas en cause l’intérêt et la réputation du GPMM, est tolérée dans les conditions définies à l’article 5 de la présente Charte, il est rappelé que les connexions établies pendant le temps de travail grâce à l’outil informatique mis à disposition par l’établissement sont présumées avoir un caractère professionnel.

Le GPMM se réserve le droit de filtrer ou d’interdire l’accès à certains sites, de procéder au contrôle a posteriori des sites visités dans les conditions définies à l’article 4 de la présente Charte. Les accès vers les sites des organismes bancaires ou institutionnels ne sont jamais analysés.

Dans le cas de tentatives ou d’agissements illicites ou frauduleux sur des sites distants, accédés via internet depuis le SI/GPMM, et si la responsabilité du GPMM était recherchée, le GPMM se réserve expressément le droit d’appliquer sans délais à l’utilisateur, les sanctions disciplinaires appropriées et d’exercer un recours contre l’intéressé au cas où sa responsabilité serait établie.

B - Messagerie électronique

Le GPMM met à la disposition des agents dont l'activité professionnelle le nécessite à des fins d'optimisation du travail, de mutualisation ou d'échange d'informations, une boîte aux lettres professionnelle nominative lui permettant d'émettre ou de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur.

Le caractère nominatif de cette adresse ne retire en rien le caractère professionnel de la messagerie.

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique du GPMM, dans les conditions définies à l'article 5 de la présente Charte.

Des adresses électroniques, fonctionnelles ou organisationnelles, peuvent être mises en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'établissement. Les utilisateurs utiliseront ce type d'adresses aux fins pour lesquelles elles ont été mises en place.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usages définies par la Direction Générale du GPMM relatives notamment à :

- la taille maximale de l'envoi d'un message,
- le nombre limité de destinataires simultanés.

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Chaque utilisateur organise et met en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou utiles dans le cadre de l'exercice de son activité professionnelle.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature, notamment ceux contraire aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par des menaces, atteinte à l'honneur par diffamation ou injure non publique, protection du droit d'auteur, protection des marques...).

L'utilisateur veille à respecter la correction normalement attendue dans tout type d'échange professionnel, écrit ou oral.

Le GPMM s'interdit d'accéder aux dossiers et aux messages identifiés comme «personnel» dans l'objet de la messagerie de l'utilisateur. Ainsi, tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

Les agents peuvent consulter leur messagerie professionnelle à distance, à l'aide d'un navigateur (webmail d'entreprise). Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'agent dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

Courriel non sollicité : filtrage par anti spam

Le GPMM dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à :

- limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres,
- ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel,
- ne pas envoyer de pièces jointes volumineuses sans autorisation préalable du destinataire,
- veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés,
- ne pas abuser des listes de diffusion ou des redirections de courrier.
- faire preuve de vigilance sur le contenu des informations reçues (désinformation, chaînes, virus informatique, tentatives d'escroquerie, etc.) et être très critique notamment sur les pétitions, alertes aux virus, retour de courriels, avis de recherche, etc. Il est conseillé aux utilisateurs à cet effet, de toujours vérifier la validité de l'information sur <http://www.hoaxbuster.com/> avant de la relayer.

Courriel avec pièces jointes dont la taille est supérieure à 10 Moctets

Le GPMM dispose d'un outil permettant d'envoyer et de recevoir des courriels dont la taille est supérieure à 10 Moctets, d'une manière sécurisée. L'usage de cet outil doit être préféré à l'utilisation d'outils gratuits proposés sur Internet.

C - Forums et réseaux sociaux

L'utilisateur doit respecter les dispositions de la « charte d'accès aux réseaux sociaux par les personnels du GPMM » annexée au présent document et celles de la présente charte.

Pour s'exprimer au nom du GPMM, ou engager celui-ci, l'utilisateur doit y avoir été dûment autorisé par un responsable-détenteur et se conformer à l'annexe «charte d'accès aux réseaux sociaux par les personnels du GPMM».

D - Téléphonie et SMS

Le GPMM peut mettre à disposition des utilisateurs, pour l'exercice de leur activité professionnelle lorsqu'elle le nécessite dans un processus d'attribution formalisé, des téléphones fixes et mobiles.

L'utilisation du téléphone fixe ou mobile (y compris rédaction de SMS) à titre privé est interdite mais peut être ponctuellement tolérée à condition qu'elle demeure raisonnable dans les conditions prévues à l'article 5 de la présente charte.

Des restrictions d'utilisation des téléphones fixes et mobiles sont mises en place en tenant compte des missions pour lesquelles ils sont affectés. A titre d'exemple, certains postes sont limités aux appels locaux, d'autres peuvent passer des appels nationaux et sur validation particulières, internationaux.

Selon les recommandations de la CNIL, il n'est pas mis en place un suivi individuel de l'utilisation des services de télécommunications autre que celui qui a trait à la facturation. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Le GPMM vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

Selon les recommandations de la CNIL, le GPMM s'interdit d'accéder à l'intégralité des numéros appelés via les autocommutateurs mis en place et via les téléphones mobiles. Hors moyens de téléphonie accordés aux représentants du personnel, en cas d'utilisation manifestement anormale, le Département du Système d'Information, sur demande d'un Directeur, se réserve le droit d'accéder aux numéros complets des relevés individuels.

Article 10 : Usage du poste de travail et des ressources informatiques

A - Sauvegardes des données professionnelles :

L'utilisateur a la responsabilité de la sauvegarde de ses données professionnelles et doit vérifier personnellement que ses données seront toujours accessibles. Le DSI propose tous les outils nécessaires aux sauvegardes mais ne peut se substituer à l'utilisateur, seul capable de déterminer l'importance et la sensibilité de chacune de ses productions.

Des sauvegardes automatiques sont réalisées en temps réel sur le poste de travail. Seuls les fichiers situés dans l'espace réservé aux fichiers professionnels (« Mes Documents ») sont sauvegardés dans un espace confidentiel sur les serveurs de fichiers du GPMM. En raison de l'espace limité par un quota, de ces sauvegardes automatiques, il est de la responsabilité de chaque utilisateur de vérifier régulièrement la complétude de celles-ci. Une note d'information spécifique exploitation (DSI/AE), disponible sur l'Intranet, fournit les outils et les éléments de compréhension nécessaires pour garantir la sauvegarde des fichiers professionnels du GPMM.

B - Chiffrement

L'utilisateur doit s'assurer qu'au moins une autre personne de son service possède les codes d'accès aux documents professionnels protégés par chiffrement. L'Autorité Qualifiée en Sécurité des Systèmes d'Information (AQSSI) peut être le dépositaire de ces codes d'accès.



Article 11 – Utilisation de l’outil informatique par les représentants du personnel

Les représentants du personnel du GPMM utilisent, dans le cadre de leur mandat, les outils informatiques et de télécommunications qui leur sont attribués pour l’exercice de leur activité professionnelle.

Les représentants du personnel du GPMM disposent d’adresses dédiées (organisation-syndicale@marseille-port.fr) et d’adresses nominatives.

Les représentants du personnel du GPMM utilisent les moyens informatiques mis à leur disposition en respectant la présente charte informatique. Par dérogation aux dispositions de l’article 4, le GPMM s’interdit d’accéder aux contenus ou informations, qui seront détruits sans être ouverts en cas d’anomalies ou incidents survenus sur le poste de travail.





Article 12 - Responsabilités- Sanctions

Il est rappelé que les droits et obligations des personnels du GPMM utilisant le système d'information du GPMM résultent de l'application de la présente charte, mais également des textes législatifs et réglementaires en vigueur applicables.

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'entraîner la mise en œuvre d'une procédure disciplinaire et d'entraîner des sanctions à l'encontre de l'utilisateur, dans les conditions prévues à l'annexe au présent document intitulée « mesures en cas de non-respect de la Charte Utilisateur ».

Il est rappelé aux utilisateurs que parallèlement à ces sanctions disciplinaires, le non-respect des textes législatifs ou réglementaires en vigueur applicables dans le cadre de l'utilisation du système d'information du GPMM (cf. rappel des principaux textes ci-après) est également susceptible de poursuites devant les tribunaux compétents.



Rappel des principales lois françaises et européennes

Toute personne sur le sol français doit respecter les règles de droit en vigueur, notamment dans le domaine de la sécurité informatique :

De nombreuses lois, encadrant l'usage des Technologies de l'Information et de la Communication, sont venues depuis une vingtaine d'années, renforcer le risque juridique. Ces lois et les codes auxquels se rattachent certaines de ces lois sont en constante évolution et la liste non exhaustive ci-dessous, n'est présentée que pour rappeler les nombreux thèmes liés à l'usage de l'informatique et traités par le législateur.

Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Loi n°1978-17 dite CNIL, relative à la protection des données personnelles du 6 janvier 1978, modifiée par les lois n°2004-801 du 6 août 2004 et n°2018-493 du 20 juin 2018.

Loi n°1990-1170 du 29 décembre 1990 concernant la **cryptologie** et l'article 28 modifié le 26/7/1996.

Loi n°2004-575 dite LCEN pour « Loi de la confiance dans l'économie numérique » du 21 juin 2004.

Loi n°2009-669 dite HADOPI pour « Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet » du 12 juin 2009.

Code pénal (Chapitre III du Titre II du Livre III) : Loi n°88-19 du 5 janvier 1988 dite **Godfrain** relative à la **fraude informatique**, modifiée par la loi n°2012-410, avec les articles 323-1 à 323-3 encadrant les intrusions dans un Système de Traitement Automatisé de Données (STAD). **Loi n° 91-646** du 10 juillet 1991 modifiée par la **Loi n° 2013-1168** du 18 décembre 2013 et notamment l'article 226-15 sur l'atteinte au secret des correspondances.



Code de la propriété intellectuelle (Chapitre I du Titre III du Livre III) : **Loi n°92-597** du 1 juillet 1992 et notamment son article L.111-1, relatif aux **droits d'auteur des œuvres de l'esprit** et à la propriété intellectuelle et complété par la **Loi n°94-361** du 10 mai 1994 sur le cas des logiciels. Voir notamment l'article R. 335-5 du code de la propriété intellectuelle. **Loi n°2006-961 dite DADVSI** relative au « droit d'auteur et aux droits voisins dans la société de l'information » du 1er août 2006

Code des Postes et des Communications Électroniques (Chapitre II du Titre I du Livre II).: Article L34-1 modifié par la **Loi n° 2013-1168** du 18 décembre 2013 sur l'obligation de **conservation des traces de connexions** permettant une communication en ligne par l'intermédiaire d'un accès réseau. **Loi n° 2004-669** du 9 juillet 2004 relative aux **communications électroniques** et aux services de communication audiovisuelle.

Code de la sécurité intérieure (Chapitre III du Titre II du Livre II) : **Loi n°73** du 21 janvier 1995 sur la **vidéosurveillance**. **Loi n°2006-64** du 23 janvier 2006 relative à la **lutte contre le terrorisme** et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers et notamment les dispositions relatives aux traitements automatisés de données à caractère personnel. **Loi n°2011-267 dite LOPPSI** pour « Loi d'orientation et de programmation pour la performance de la sécurité intérieure » du 14 mars 2011.

Annexes

Signature de la Charte Utilisateur



Je soussigné Monsieur, Madame, Mademoiselle,
exerçant les fonctions de :

au sein de la Direction / Département / Mission / Activité

étant à ce titre amené à accéder au Système d'Information du Grand Port Maritime de Marseille, reconnaît avoir pris connaissance de la Charte Utilisateur, ci-annexée et en avoir compris les exigences, mais aussi les droits et les devoirs.

La CNIL (Commission Nationale Informatique et Libertés) recommande l'adoption d'une charte dans l'entreprise ayant pour objectif de « sensibiliser les salariés » aux exigences de sécurité, d'appeler leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'entreprise. Notre charte a ainsi pour objectif d'établir un cadre clair et transparent des règles d'utilisation de l'informatique et d'Internet au sein du GPMM afin de maîtriser les risques liés à l'utilisation du Système d'Information (SI) par les salariés.

La charte impose au salarié plusieurs obligations mais accorde aussi des droits :

- La charte applique la présomption selon laquelle les outils mis à disposition par l'employeur sont à vocation professionnelle, mais rend possible une utilisation personnelle à condition qu'elle soit raisonnable. Il appartient, au salarié, notamment de distinguer les documents ou e-mails qu'il considère comme personnels, des documents professionnels. Tout document ou e-mail qui ne comporterait pas cette distinction personnelle sera alors considéré comme professionnel. Le salarié doit également s'engager à ne pas transformer des informations professionnelles en informations personnelles.
- La charte prévoit également que pour des motifs de protection destinés à assurer le bon fonctionnement du SI, le contrôle pourra être exercé par l'employeur en termes notamment de volumes et d'outils installés sur le poste de travail. Le contrôle du contenu sera limité à des cas exceptionnels, nécessités par l'urgence ou par un comportement qui serait pénalement sanctionnable.
- La charte rappelle au salarié la nécessité de respecter l'environnement légal applicable, et notamment au regard des droits des tiers et de l'entreprise, tels que la confidentialité et le respect des droits d'auteur.
- Un salarié se voit attribuer un identifiant et un mot de passe pour accéder au SI. Il devra respecter l'usage de cet identifiant et de ce mot de passe et en protéger la confidentialité.

Les utilisateurs du Système d'Information du Grand Port Maritime de Marseille disposent conformément au règlement général sur la protection des données (RGPD) applicable le 25 mai 2018, d'un droit à l'art. 15 de rectification art. 16 de suppression art. 17 d'un droit d'opposition art. 21, des données à caractère personnel les concernant.
Des droits peuvent être exercés sous réserve de la fourniture d'une pièce justificative d'identité et d'un motif légitime auprès du responsable de la protection des données du GPMM, car mail : protection@gpmm.fr

Grand Port Maritime de Marseille
23, place de la Joliette - BP 31965 - 13226 Marseille Cedex 03
Tél : 04 91 39 40 00 - Fax : 04 91 39 57 00
www.marseille-gpmm.fr





La charte impose que l'accès aux ressources informatiques ne pourra se faire qu'après acceptation des modalités convenues dans la charte, et que le non-respect des dispositions de la charte engagera la responsabilité du salarié.

Je m'engage, en tant qu'utilisateur du SI du GPMM, dans la limite de mes attributions et des moyens mis à ma disposition, conformément au Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à prendre toutes précautions conformes aux usages et à l'état de l'art afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient modifiées, endommagées ou communiquées à des personnes non expressément autorisées à recevoir ces informations.

Ayant pris connaissance des conditions d'usage de l'Internet et des contrôles qui peuvent être faits, je m'engage à respecter cette Charte.

Tout non-respect pourra conduire le GPMM à supprimer mon droit d'accès au Système d'Information du GPMM et pourra conduire le GPMM à recourir à des sanctions disciplinaires à mon encontre.

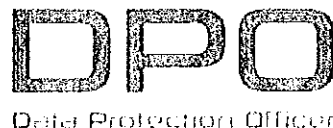
Fait à Marseille, le

Les utilisateurs du Système d'Information du Grand Port Maritime de Marseille disposent conformément au règlement général sur la protection des données 2016/679 approuvé le 25 mai 2016, d'accès à : 15. de rectification ; art. 16. de suppression ; art. 17. d'un droit d'opposition ; art. 21. des données à caractère personnel les concernant. Ces droits peuvent être exercés sous réserve de la fourniture d'une pièce justificative d'identité et d'un motif légitime auprès du délégué à la protection des données du GPMM par mail à adresser à : dpd@marseillesp.fr

Grand Port Maritime de Marseille
25, place de la Joliette - BP 51965 - 13226 Marseille Cedex 02
Tél : 04 91 39 40 00 - Fax : 04 91 39 57 00
www.marseillesp.fr



Engagement de confidentialité « Données à caractère personnel »



Engagement de confidentialité « Données à caractère personnel »

Je soussigné Monsieur, Madame, Mademoiselle,
exerçant les fonctions de :

.....
au sein de la Direction / Département / Mission / Activité

....., du Grand Port Maritime de Marseille,

étant à ce titre amené à accéder à des données à caractère personnel, déclare reconnaître la confidentialité des dites données.

Je m'engage par conséquent, conformément au règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient modifiées, endommagées ou communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions et traiter chaque copie avec le même degré de confidentialité que son original ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité matérielle de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- assurer, dans la limite de mes attributions, l'exercice des droits d'information, d'accès et de rectification de ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, les copies, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel. J'ai été informé que toute violation du présent engagement m'expose notamment à des actions et sanctions disciplinaires et pénales conformément aux dispositions légales en vigueur.

Fait à Marseille, le... / ... / 201...



Engagement de confidentialité pour les informaticiens



Marseille, le... / ... / ...

Je soussigné Monsieur, Madame, Mademoiselle
exerçant les fonctions¹ de :
au sein² de : du **Grand Port Maritime de Marseille**,
étant à ce titre amené, dans le cadre de mes fonctions, à accéder à des données techniques ou
à caractère personnel, déclare reconnaître la confidentialité des dites données.

Je m'engage par conséquent, conformément au règlement UE 2016/679 du 27 avril 2016 relatif
à la protection des personnes physiques à l'égard du traitement des données à caractère
personnel, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre
de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et
en particulier d'empêcher qu'elles ne soient modifiées, endommagées ou communiquées à des
personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles
prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs
fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques,
physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution
de mes fonctions et traiter chaque copie avec le même degré de confidentialité que son
original ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de
mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la
sécurité matérielle de ces données (notamment les journaux de logs) ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication
sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers
informatiques et tout support d'information relatif à ces données.
- alerter sans délais ma hiérarchie et/ou l'AQSSI/DPO de toutes les anomalies mettant
en jeu la sécurité et pour tous les risques relevant du règlement UE 2016/679 du 27 avril
2016.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions,
demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en
soit la cause. Je suis informé que toute violation du présent engagement m'expose notamment
à des actions et sanctions disciplinaires et pénales conformément aux dispositions légales en
vigueur.

Fait pour valoir ce que de droit

¹ Administrateur système, Administrateur réseau, Développeur, Atelier Micro, Chef de projet informatique,
Urbaniste technique des données, Gestionnaire d'Application, Administrateur système industriel,
Administrateur site web

² DAF/DSI/AD, DAF/DSI/AE, DAF/DSI/AEI, DAF/DSI/ATR, DA/DGT/ASI, DD/DCRE/AC

Grand Port Maritime de Marseille
23 place de la Joliette - BP 51965 - 13226 Marseille Cedex 02
Tél : 04 91 39 46 00 - Fax : 04 91 39 57 00
gpm@marseille-gpm.fr - www.marseille-gpm.fr





Charte d'accès aux réseaux sociaux par les personnels du GPMM

Définitions

Utilisateur : toute personne, employé du GPMM, étant inscrite sur le site d'un «réseau social» et pouvant publier des contributions.

Contribution : les commentaires et éléments/contenus (vidéos, photos, dessins, musique, liens hypertextes...) pouvant être publiés par les utilisateurs d'un «réseau social».

Champ d'application

L'utilisateur, par le fait de contribuer par la rédaction d'articles, de commentaires sur la page d'un «réseau social» au titre de son appartenance au GPMM, accepte pleinement et sans aucune réserve la présente charte d'utilisation, et s'engage, lors de chacune de ses visites sur la page d'un «réseau social», à respecter les principes et l'esprit des recommandations de la présente charte d'utilisation.

L'utilisation à des fins privées, notamment en ne faisant pas apparaître son appartenance au GPMM, de services gratuits disponibles sur Internet n'entre pas dans le champ de la présente charte, se réalise sous l'entière responsabilité de son auteur et à ce titre, n'est pas autorisée à partir du réseau du GPMM.

L'utilisation à des fins professionnelles de services gratuits disponibles sur Internet (forum de discussion, outils collaboratifs sur des sites de réseaux sociaux ...) suscite de manière générale de sérieuses réserves.

En effet, l'usage professionnel d'un service doit être encadré par un contrat détaillant les mesures destinées à assurer la protection des informations mais aussi à garantir le GPMM et ses agents contre toutes les conséquences de l'usage du service. En absence de contrat, aucune garantie ne peut être exigée et les risques sont accrus lorsque le fournisseur du service est situé à l'étranger. La lecture attentive et répétée ainsi que la compréhension précise des CGU décrites chez les fournisseurs de services gratuits conduisent le GPMM à étudier au cas par cas l'opportunité de proposer de tels services à ses agents.



Un «réseau social» professionnel type LinkedIn, Viadeo, Xing ou autre a pour objectif de développer une communauté internet conviviale autour d'un thème et de son actualité, et de donner l'occasion à cette communauté de se rencontrer au sein d'un espace public d'échange d'opinions, d'idées ou de connaissances.

La présente Charte d'utilisation a été élaborée afin de préciser aux agents du GPMM, amenés à participer à un projet collaboratif avec des entreprises ou organismes externes, les conditions pour une utilisation conforme aux intérêts de l'agent et du GPMM lors des accès aux espaces d'échanges d'un «réseau social». Ainsi, le droit du travail reconnaît à l'employé le droit de s'exprimer librement, tant à l'intérieur qu'à l'extérieur de son lieu de travail, au sujet de son employeur.

Toutefois ce droit ne peut être exercé de manière abusive, d'autant plus que l'employé est soumis à une obligation légale d'exécuter son contrat de travail avec loyauté. En effet, l'employé pourra se voir reprocher de publier des contributions sur le fonctionnement de son entreprise ou sur ses conditions de travail, sur ses collègues ou sa hiérarchie si ces publications relèvent du dénigrement, de la diffamation ou de l'injure publique.

Bonnes pratiques d'usage d'un « réseau social »

Dans le cas d'un usage privé, réalisé à partir d'un poste situé hors du réseau GPMM, il est fortement recommandé aux agents du GPMM de se protéger, en appliquant ces bonnes pratiques : en effet le « droit à l'oubli » est une notion tout à fait relative dans la sphère Internet, où il est extrêmement difficile d'obtenir la suppression de contributions « embarrassantes ».

Lors de l'inscription :

L'accès à un « réseau social » est libre. Pour y publier des contributions, l'utilisateur doit s'être inscrit au préalable sur le site internet du « réseau social », dans le respect des conditions générales d'utilisation (CGU) de ce site que l'utilisateur doit lire attentivement en vérifiant, notamment :

- la possibilité de suppression de chacune de ses contributions par lui-même ou par le modérateur du site,
- l'éventuelle interdiction d'un usage professionnel,
- l'éventuelle possibilité pour l'hébergeur d'exploiter les contenus mis en ligne par les utilisateurs,
- la possibilité et les conditions de désinscription
- les conséquences des évolutions fréquentes des CGU.

L'utilisateur doit avoir conscience que ses contributions (messages et/ou contenus) peuvent :

- être consultées par tous les autres internautes du «réseau social» et pas seulement les destinataires auxquels il croyait s'adresser,
- être communiquées à toute autorité judiciaire ou toute autre autorité publique qui en fait la demande,
- être référencées et archivées sur un moteur de recherche, et donc, susceptibles d'être consultées par un public extérieur au site du «réseau social».

Lors de l'inscription, l'utilisateur est seul responsable de la diffusion par lui de ses données personnelles, et des conséquences de cette diffusion.

Lors des contributions :

Si l'agent, ne fait pas apparaître son appartenance au GPMM, il doit veiller à ce que ses propos :

- respectent les lois et règlements en vigueur,
- ne soient pas contraire à l'ordre public ou aux bonnes mœurs,
- ne portent pas atteinte aux droits des personnes (par exemple protection des données personnelles), au droit à l'image, au droit au respect de la vie privée,
- ne portent pas atteinte à la réputation d'une marque ou d'une personne physique ou morale
- ne reproduisent sans autorisation une œuvre protégée par des droits de propriété intellectuelle (marques, droits d'auteur et droits voisins),
- ne puissent être jugées comme :
 - étant à caractère violent, dénigrant, diffamatoire, injurieux, illicite, obscène, pornographique, pédophile, ou de nature à heurter la sensibilité;
 - étant à caractère politique ou incitant à la violence, au suicide, au révisionnisme, à l'antisémitisme, à la discrimination ou à la haine;
 - faisant l'apologie des crimes de guerre ou des crimes contre l'humanité ;
 - appelant au meurtre ou incitant à la commission d'un délit ;

Attention, l'utilisateur doit cependant prendre en compte que son appartenance au GPMM peut être connue par ailleurs. Il est donc prudent de considérer que de ne pas annoncer son appartenance au GPMM sur un réseau social, n'exonère pas l'utilisateur des recommandations suivantes.

Si, en s'inscrivant sur un «réseau social», l'utilisateur déclare son appartenance au GPMM, il engage sa responsabilité vis-à-vis du GPMM, son employeur.

Il doit d'abord décrire, en toute transparence, succinctement son rôle au sein de l'entreprise afin de faire comprendre, au mieux, la teneur de ses contributions.

Sur la forme du contenu, il lui est conseillé d'adopter une attitude professionnelle, respectueuse et courtoise, en effet ses contributions reflètent l'image du GPMM.

Sur le fond, ses publications sur un réseau social, doivent éviter d'entraîner tout conflit notamment de nature personnelle et ne doivent pas laisser apparaître un manque de loyauté envers son employeur.

Afin d'éviter toute pratique trompeuse vis-à-vis des lecteurs du « réseau social », l'utilisateur doit veiller notamment à ce que le contenu de ses contributions montre clairement qu'elles exposent ses opinions personnelles et non pas celles du GPMM. L'utilisateur doit, pour cela, utiliser systématiquement la première personne du singulier.

Enfin, en cas de doute, si l'agent n'est pas sûr de savoir si la divulgation de certaines informations professionnelles en sa possession pourrait nuire à l'entreprise, il doit, avant de les publier, demander son avis à son supérieur hiérarchique ou à l'AQSSI-DPO du GPMM.

Contributions par un agent dans le cadre d'un « projet GPMM »

Les recommandations du chapitre précédent deviennent des exigences. Les contributions de l'utilisateur étant réalisées à partir d'un poste situé sur le réseau du GPMM, les devoirs et obligations de la charte utilisateur, annexe du contrat de travail, s'appliquent pleinement et sans restriction.

Chaque projet GPMM est conduit par un responsable du projet appelé **responsable-détenteur** (liste des responsables-détenteur sur l'intranet), le plus souvent cadre du GPMM.

Le projet nécessite, à la demande du responsable-détenteur du projet, l'ouverture d'un accès vers le « réseau social » par le département du Système d'Information.

L'usage de réseaux sociaux, doit être modéré, par le responsable-détenteur du projet qui :

- détermine le niveau de « sensibilité » des informations, les risques acceptables et les conditions d'accès par les utilisateurs concernés du GPMM,
- est responsable, dans le cadre du projet, des publications et contributions réalisées par les agents du GPMM sur le «réseau social»,
- est l'interlocuteur privilégié des activités opérationnelles DSI/ATR, DSI/AE qui doivent obtenir son accord avant tout changement concernant l'accès au « réseau social » depuis un poste du GPMM et l'affectation des droits d'accès aux agents concernés par le projet.

Le responsable-détenteur est garant de la sécurité du patrimoine informationnel de son périmètre. Il définit avec les agents qu'il a désignés dans le cadre du projet, le contenu et la forme des contributions qu'ils sont autorisés à publier sur le « réseau social » concerné et dont l'accès est autorisé depuis le réseau du GPMM.

Afin de lui permettre d'exercer pleinement ses responsabilités, le responsable-détenteur du projet définit, en fonction de la sensibilité des informations manipulées et du risque associé à leur divulgation, les conditions de contribution des utilisateurs du GPMM qu'il a désignés :

- Soit les utilisateurs, accèdent au « réseau social » par un compte unique appelé « GPMM-NOM-DU-PROJET » dont le mot de passe est connu du responsable-détenteur. Ainsi, le responsable-détenteur et chacun des utilisateurs désignés peuvent intervenir sur le site du « réseau social » pour ajouter une contribution nécessaire ou pour enlever une contribution inopportune.
- Soit les utilisateurs, accèdent au « réseau social » par un compte personnel de la forme « prenom.NOM-GPMM » dont le mot de passe est connu de lui seul. Dans ce cas, l'utilisateur assume seul la responsabilité de ses contributions. Il est en effet le seul à pouvoir intervenir sur le site du « réseau social » pour ajouter ou enlever une de ses contributions.

Lors de l'inscription sur le site d'un « réseau social », une adresse mail de secours est souvent requise pour permettre au responsable du site, d'assurer la gestion des « mots de passe oubliés ». Cette procédure doit pouvoir être conduite même en cas d'indisponibilité des contributeurs. Il convient de fournir l'adresse professionnelle du responsable-détenteur.



Mesures en cas de non-respect de la Charte Utilisateur

L'utilisation faite des moyens informatiques que le GPMM met à la disposition de ses agents, déroge parfois aux règles de sécurité mises en place. Ces règles sont rappelées lors de chaque ouverture de session et sont décrites dans la charte utilisateur.

Des cas d'utilisation non-conforme ont déjà été détectés. Des sanctions ont été prises à l'encontre des auteurs.

Il s'agit de formaliser, de manière objective, les éléments permettant d'établir le cas de non-respect et de proposer les « suites à donner ».

Le comportement non-conforme peut être signalé de plusieurs manières :

- Informations recueillies auprès d'autres agents GPMM,
- Informations reçues de l'extérieur (Police, CERTA, ANSSI, ...),
- Signaux consécutifs à une attaque via un malware importé depuis une clé USB, ou une pièce jointe dans un mail ou encore après avoir cliqué sur un lien piégé,
- Détection par les outils d'analyse (installation et utilisation de logiciel....)

Conformément aux exigences réglementaires, les outils de surveillance du GPMM enregistrent toutes les actions réalisées sur le SI :

- Outil d'analyse comportementale
 - Logiciel Nexthink qui trace et conserve pendant 4 mois toutes les activités applicatives et logicielles des postes de travail. Cet outil propose des statistiques et dispose d'un moteur d'analyse capable à partir d'une base de connaissance de repérer tout comportement anormal d'un poste de travail.
 - L'AQSSI, l'ASSI et les agents DSI/AE et ART consultent le portail de Nexthink pour confirmer les signaux reçus par les outils décrits ci-après.
- Outils Exploitation
 - Analyse des logs des serveurs, actuellement manuelle par les administrateurs DSI/AE
- Outils Réseaux
 - Analyse des logs des équipements réseaux, actuellement manuelle par les administrateurs DSI/ART

Les agents de DAF/DSI assurent chacun en ce qui le concerne, la surveillance du bon fonctionnement du Système d'Information :

- Activité Exploitation : Hotline, Atelier Micro et les administrateurs système
- Activité Réseaux et Télécommunication : Réseau et sécurité



Les agents DSI analysent les résultats fournis par les outils décrits au point précédent, et détectent les comportements atypiques par :

- L'utilisation de programmes :
 - inhabituels (non validés par DSI)
 - connus comme étant dangereux
- Consommations excessives de ressources
- Accès à des sites suspects (par exemple ceux proposant des outils de hacking)

Bien entendu, les agents du DSI sont formés pour détecter les faux positifs (alarmes injustifiées), notamment en procédant à une analyse croisée des différentes sources d'information afin de réduire le risque de mauvaise interprétation.

Motivation des comportements non conformes

Il convient de comprendre les raisons d'un comportement atypique. Il est toujours possible d'imaginer que le comportement est dû, par exemple et notamment, à :

- une erreur dans l'interprétation de l'alerte,
- une erreur ponctuelle et involontaire → à expliquer si grave ou trop fréquente,
- une curiosité légitime → à encourager en refixant le cadre,
- une curiosité excessive et/ou volontaire → à décourager,
- une activité sans limite sur les téléchargements (comme à la maison) → à décourager,
- une volonté de contourner la charte informatique pour améliorer sa productivité → à décourager en proposant des solutions validées,
- une volonté de contourner la charte informatique pour obtenir un gain → à sanctionner,
- une volonté de nuire (destruction, divulgation, piratage...) → à sanctionner.

Une analyse des informations données par les outils de surveillance se doit d'être confirmée ou infirmée par un entretien avec l'utilisateur. Cet entretien permet de comprendre les éventuelles motivations ainsi que la volonté de masquer ses actions ou celle d'éclairer la situation.

Un compte-rendu doit être rédigé. Ce compte-rendu est envoyé, sous couvert de la voie hiérarchique, par mail pour être tracé.

Les échelles : Gravité et Intentionnalité

La définition des termes utilisés ci-dessous est consultable dans le glossaire en fin de document.

Echelle de gravité de l'impact	Graduation	Exemples de description des impacts et des risques
A, Mineur	Pas de conséquences de l'impact pour le GPMM	Aucun impact sur la sécurité du SI, aucune charge DSI
B, Modéré	GPMM surmontera les conséquences de l'impact sans difficulté.	<u>Risque</u> d'atteinte à la sécurité du SI, charge DSI modérée,
C, Important	GPMM surmontera les conséquences de l'impact avec quelques difficultés.	Atteinte à la sécurité du SI, charge DSI significative, <u>Risque</u> d'atteinte à l'image de marque du GPMM
D, Critique	GPMM surmontera les conséquences de l'impact avec de sérieuses difficultés.	Atteinte à l'image de marque du GPMM, divulgation avérée de données sensibles, atteinte à un élément du SI, plan d'actions DSI perturbé, contournement des barrières de sécurité.

Echelle de degré d'intentionnalité	Graduation	Exemples de description des explications données et de l'attitude
1, Insouciance	Ignorance de la charte Informatique et plus généralement des bons usages de l'outil Informatique	Insouciance, Non conscience des conséquences, Erreur. Action involontaire
2, Curiosité	Omission de la charte Informatique pour rechercher de nouveaux outils améliorant la productivité	Curiosité, manipulation extérieure. Action ponctuelle
3, Délibérée	Recherche de contournement des outils de sécurité du Port pour obtenir un avantage	Volontaire, compétence limitée. Actions simples répétées
4, Malveillante	Volonté de nuire	Volontaire, compétence avérée. Actions complexes répétées

Les 2 situations possibles

Les risques classés en rouge sont jugés **intolérables**.

Les risques classés en orange sont jugés **importants**.

Les risques classés en jaune sont jugés **significatifs**.

Les risques classés en vert sont jugés **négligeables**.

Premier constat

Gravité	D, Critique	D1	D2	D3	D4
	C, Importante	C1	C2	C3	C4
	B, Modérée	B1	B2	B3	B4
	A, Mineure	A1	A2	A3	A4
		1, Insouciance	2, Curiosité	3, Délibérée	4, Malveillante
Intention					

En cas de récurrence

Les risques sont aggravés en cas de récurrence.

Gravité	D, Critique	D1'	D2'	D3'	D4'
	C, Importante	C1'	C2'	C3'	C4'
	B, Modérée	B1'	B2'	B3'	B4'
	A, Mineure	A1'	A2'	A3'	A4'
		1, Insouciance	2, Curiosité	3, Délibérée	4, Malveillante
Intention' (récurrence)					

Proposition de suites à donner

Selon la classification retenue (de A à D et de 1 à 4) et le critère de gestion de risque affecté (de vert à rouge), le traitement doit être proportionné au caractère de la faute.

La sanction est toujours du ressort de la DG, assistée de la DRH et de la DAJ.

Le signalement de la faute auprès de la DRH, de la DAJ et du DG est systématique sauf si le risque évalué est considéré comme négligeable.

Ce signalement est obligatoire si le comportement :

- Est volontaire et contraire à la Charte Informatique,
- Entraîne un risque de sécurité (juridique, technique, financier, image de marque...),
- Démonstre une activité non déontologique,
- Porte atteinte à la sécurité du SI.

Au sein du DSI, les agents, les responsables d'activités et le chef de département sont les premiers informés des cas d'utilisation anormale. Après analyse, ils informent l'AQSSI, chargé de mener une investigation auprès de l'auteur, d'informer par un compte-rendu, sa hiérarchie, le département DRH/DS et la DG.

Notamment, en cas de déni, mais aussi quand les preuves de l'action (traces contenues dans le poste de travail) doivent être conservées de manière à être ultérieurement opposable, la protection des preuves doit être mise en place.

Sur décisions de la Direction Générale, la DAJ prend en charge l'appel à un huissier, qui convient d'un rendez-vous pour saisir le poste en présence de l'AQSSI. Un CR est rédigé, par l'AQSSI, à l'issue de la saisie, le poste est conservé par l'huissier pour une éventuelle expertise.

L'attention du lecteur est attirée sur le caractère parfois insuffisant des preuves « informatiques ». Par exemple, lorsqu'un mot-de-passe est divulgué, il n'est plus possible de connaître le vrai auteur d'une faute.

Risques négligeables

Dans la plupart des cas rencontrés, il s'agit d'un utilisateur qui n'a fait l'objet d'aucune alerte antérieure et la gravité apparaît faible :

Un simple appel téléphonique de la part de l'agent DSI qui a constaté l'anomalie suffit à réduire le risque. Un mail de rappel à l'ordre lui est envoyé.

Si la volonté de l'agent de contourner la Charte Informatique semble plus probable, le supérieur hiérarchique de l'agent peut être appelé par le responsable DSI/ATR ou AE. La DRH n'est pas systématiquement informée.

Risques significatifs

Si le responsable DSI/ATR ou AE le juge nécessaire, notamment suivant la gravité des faits constatés, l'ASSI, le Chef de Département du SI et l'AQSSI sont informés et l'AQSSI prend les mesures nécessaires :

Appel de l'agent mis en cause pour lui confirmer la gravité des faits reprochés, puis appel de son supérieur hiérarchique.

Ces appels sont accompagnés d'un mail de confirmation rappelant les faits. La DRH est systématiquement informée.

Risques importants ou critiques

Niveau de gravité A ou B :

L'ASSI (Responsable de l'activité DSI/AE) ou le Chef du Département du SI alertent l'AQSSI qui informe la DRH, la DAJ et la DG. La mise sous séquestre (Huissier) est demandée.

Ni l'agent suspecté ni son supérieur hiérarchique ne sont informés avant une prise de décision par la DRH, la DAJ et la DG.

Niveau de gravité C ou D :

L'ASSI (Responsable de l'activité DSI/AE) et le Chef de département du SI prennent les mesures nécessaires pour maintenir (ou remettre) le SI en condition opérationnelle (PCA et PRA). Le Chef de département du SI alerte l'AQSSI qui informe la DRH, la DAJ et la DG.

La cellule de gestion de crise* (règle n°3 de la PSSI) est actionnée. Une information préalable est remontée au FSSI et à l'ANSSI avec mise sous séquestre (Huissier de justice avec aide technique de l'ANSSI pour mieux préserver les traces). Ni l'agent suspecté ni son supérieur hiérarchique ne sont informés avant une prise de décision par la cellule de gestion de crise.

[*] Composée de : Chefs de département DSI, DSD, Responsables d'activité AE et ART, AQSSI et experts choisis.

Glossaire

AQSSI Autorité Qualifiée en Sécurité des Systèmes d'Information

ANSSI Agence Nationale SSI (service du Premier Ministre)

DPO Data Protect Officer /Délégué à la protection des données (ex CIL)

DSI Département du Système d'Information

FSSI Fonctionnaire SSI rattaché au HFD

HFD Haut-Fonctionnaire de Défense du Ministère de Tutelle

PSSI Politique de Sécurité des Systèmes d'Information

SI Système d'information

Action délibérée : fait d'agir après avoir réfléchi (avec soi-même). L'action est composée d'un enchainement de tâches à accomplir (par exemple installation d'un logiciel).

Action involontaire : fait d'agir sans le contrôle de sa volonté.

Action ponctuelle : fait d'agir une seule fois.

Actions répétées : fait d'agir identiquement à plusieurs reprises.

Action volontaire : fait d'agir avec le contrôle de sa volonté.

Code ou logiciel malveillant : Code ou logiciel développé dans le but de nuire à un SI. Les virus, vers, chevaux de Troie ou bombes logiques constituent des exemples de codes ou de logiciels malveillants.

Compétence avérée : Disposant de diplôme en Informatique, occupant ou ayant occupé un poste dans un service informatique.

Compétence limitée : utilisateur standard ne disposant pas de compétences avérées.

Curiosité : Désir d'apprendre, d'améliorer ses connaissances techniques.

Données à caractère personnel : Des données sont considérées comme à caractère personnel dès lors qu'elles permettent d'identifier directement ou indirectement des personnes physiques.

Erreur : faute commise en se trompant, maladresse, action regrettable. En droit, vice du consentement pouvant entraîner la nullité d'un acte.

Ignorance : par manque de connaissances, ne pas connaître quelque chose dans un domaine particulier, ne pas être au courant, incompétence dans un domaine précis.

Insouciance : caractère de celui qui ne se soucie de rien, imprévoyance.



Manipulation extérieure : sous l'emprise d'une force extérieure à l'entreprise.

Obtention d'un avantage : L'action commise procure un gain (financier, connaissance d'une information sensible, technique ou à caractère personnel ...).

Personne malveillante : personne qui exprime, par ses actions, une intention de faire du mal, de nuire, à l'entreprise ou à un agent.

Poste nomade ou mobile : Ensemble des ressources mobiles du système d'information ou des ressources permettant l'utilisation du système d'information avec des ressources mobiles. Par exemple : assistants personnels, ordinateurs portables, téléphones portables de type Smartphones, accès wifi, ...

Recherche de contournement des outils de sécurité du Port : Pour masquer ses actions ou pour accéder à des ressources non autorisées (sites internet, fichiers sur le réseau, usage non-conforme de mots de passe).

Recherche de nouveaux outils améliorant la productivité : usage d'outils non validés par DSI mais offrant des fonctionnalités professionnelles.

Responsable de traitement : La Directrice Générale, Présidente du Directoire.

Responsable-détenteur d'une application : Responsable métier garant du patrimoine informationnel de l'application, qui détermine le niveau de «sensibilité», les risques acceptables, les conditions d'accès et de mise à jour des informations. C'est l'interlocuteur privilégié de DSI.

Système d'information : Ensemble des ressources techniques, applicatives, organisationnelles, humaines et documentaires permettant de collecter, stocker, traiter, rechercher et/ou transmettre des données, en particulier :

- Tout matériel informatique fixe : postes (dont les postes libre-service), serveurs, téléphones, périphériques (clavier, écran, imprimante, etc.), prises, câbles, ...
- Tout matériel informatique mobile : ordinateur, téléphone, etc.
- Tout logiciel ou service réseau ou informatique : accès réseau, accès internet, messagerie électronique, bureautique, etc.
- Tout support de données : électronique, papier, etc.

Utilisateur : désigne toute personne autorisée à accéder au système d'information en général de quelque manière que ce soit (par lien filaire ou hertzien) et en particulier aux outils informatiques et aux moyens de communication du GPMM et à les utiliser : employés, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels...

Volonté de nuire : chercher à provoquer un impact significatif (juridique, financier, industriel, commercial).

Table des matières

Préambule	3
Article 1 - Champ d'application.....	5
Article 2 - Conditions d'accès (sur un poste utilisateur)	7
Article 3 – Règles générales d'utilisation, de sécurité et de bon usage	9
A – Sur son poste de travail.....	9
B - Equipements nomades d'entreprise	11
C - Procédures spécifiques aux matériels de prêt.....	12
Article 4 - Contrôle, imputabilité et traçabilité des actions.....	13
A - Les systèmes automatiques de filtrage.....	14
B - Les systèmes automatiques de traçabilité.....	14
C – La surveillance du poste de travail	14
Article 5 - Utilisation des moyens informatiques à des fins privées.....	15
Article 6 - Respect des droits de propriété intellectuelle	17
Article 7 - Protection des données à caractère personnel (DCP)	19
Article 8 – Gestion des absences et des départs.....	21
Article 9 – Règles particulières relatives à l'usage des services Internet, messagerie, forum, téléphonie.....	23
A - Internet	23
B - Messagerie électronique	24
C - Forums et réseaux sociaux	26
D - Téléphonie et SMS	26
Article 10 : Usage du poste de travail et des ressources informatiques.....	27
A - Sauvegardes des données professionnelles :	27
B - Chiffrement	27
Article 11 – Utilisation de l'outil informatique par les représentants du personnel	29
Article 12 - Responsabilités- Sanctions	31
Rappel des principales lois françaises	33

Annexes	35
Signature de la Charte Utilisateur	35
Engagement de confidentialité « Données à caractère personnel »	37
Engagement de confidentialité pour les informaticiens	39
Charte d'accès aux réseaux sociaux par les personnels du GPMM	41
Définitions	41
Champ d'application.....	41
Bonnes pratiques d'usage d'un « réseau social »	43
Contributions par un agent dans le cadre d'un « projet GPMM »	46
Mesures en cas de non-respect de la Charte Utilisateur	49
Motivation des comportements non conformes	50
Les échelles : Gravité et Intentionnalité.....	51
Les 2 situations possibles	52
Proposition de suites à donner	53
Risques négligeables	54
Risques significatifs	54
Risques importants critiques	54
Glossaire	55