2021-2023

Charte Informatique

École française d'Athènes

Préambule

La présente charte est portée à la connaissance de tout utilisateur des technologies de l'information et de la communication (TIC) à l'École française d'Athènes (EFA).

Elle définit les règles régissant l'usage des TIC et les règles de sécurité du système d'information que l'utilisateur et l'institution s'engagent à respecter et précise les droits et devoirs de chacun.

Par ***système d'information*** s'entend l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition de l'***utilisateur***.

L'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portables ... sont également des éléments constitutifs du système d'information.

Par ***utilisateur***, s'entend toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut.

Ainsi sont notamment désignés :

- Tout agent titulaire ou non-titulaire, vacataire, stagiaire.
- Tout prestataire ayant contracté avec l'établissement.
- Toute personne : hébergée à la maison des hôtes, lecteur de la bibliothèque, doctorants, invité…

Par **adresse électronique de fonction**, s'entend une messagerie électronique comprenant l'ensemble du système permettant la transmission et réception de courrier électronique. Elle est nominative lorsqu'elle composée du prenom.nom@efa.gr de l'utilisateur, mais peut aussi correspondre à un service ou à une fonction dès lors qu'il répond à un besoin défini. Dans ce dernier cas, l'adresse peut être partagée par plusieurs utilisateurs.

Par **adresse électronique privée**, s'entend toute messagerie électronique n'étant pas hébergée par l'EFA (type Orange, OteNet, Gmail, etc ..), qui doit être utilisé à des fins privées et non professionnelles.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent et notamment, la sécurité, la performance des traitements et la conservation des données personnelles.

Engagements de l'École française d'Athènes

L'EFA met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'EFA facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel, mais l'École française d'Athènes est tenue de respecter la vie privée de chacun.

Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.

Les utilisateurs ont une responsabilité particulière dans l'utilisation qu'ils font des ressources mises à leur disposition par l'EFA. En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

ARTICLE I. CHAMP D'APPLICATION

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'École française d'Athènes ainsi qu'à l'ensemble des utilisateurs.

ARTICLE II. CONDITIONS D'UTILISATION DES SYSTÈMES D'INFORMATION

Section II.1 Utilisation professionnelle / privée

Les communications électroniques (utilisation des ressources informatiques, usage des services Internet, usage du réseau) sont destinées à l'activité professionnelle des utilisateurs. L'activité professionnelle doit être entendue comme celle définie par les textes spécifiant les missions du service public de l'enseignement supérieur, à savoir :

1 – La formation initiale et continue.

2 – La recherche scientifique et technologique, la diffusion et la valorisation de ses résultats.

3 – L'orientation et l'insertion professionnelle.

4 – La diffusion de la culture et l'information scientifique et technique.

5 – La participation à la construction de l'Espace européen de l'enseignement supérieur et de la recherche.

6 – La coopération internationale.

Elles peuvent cependant constituer le support d'une communication privée. L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans la fréquence que dans la durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des systèmes d'information doit demeurer négligeable au regard du coût global d'exploitation.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement (par exemple, cet espace pourrait être dénommé « privé » ou « personnel ») à cet effet ou en mentionnant le caractère privé sur la ressource. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

Plus concrètement :

– Il est donc interdit de stocker des données à caractère privé sur des disques réseau, des plateformes applicatives ou bien des ressources Web appartenant à l'EFA.

– Le service informatique se réserve le droit de supprimer toutes les données ne respectant pas ce principe.

– L'EFA ne peut pas être tenu responsable de la perte des données à caractère privé.

Section II.2 Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer cette continuité, l'utilisateur devra toujours utiliser, pour les activités liées à sa fonction, une adresse électronique de fonction et les espaces partagés mis à sa disposition.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace. Dans le cas où cet espace de données à caractère privé n'aurait pas été détruit par l'utilisateur, l'établissement s'engage à ne divulguer aucun des éléments y figurant à des tiers, sauf cas prévus par la réglementation.

En ce qui concerne la messagerie l'utilisateur pourra demander à y accéder pendant une durée de 1 mois après son départ définitif, au-delà, les données seront détruites.

L'utilisateur doit garantir l'accès à tout moment à ses données professionnelles. En cas d'absence non planifiée et pour des raisons exceptionnelles, si un utilisateur se trouve dans l'obligation de communiquer ses codes d'accès au système d'information, il doit procéder dès que possible au changement de ces derniers ou en demander la modification au service informatique.

Section II.3 Utilisation conforme aux lois en vigueur

a) Respect de la propriété intellectuelle

L'EFA rappelle que l'utilisation des moyens informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits. En conséquence, chaque utilisateur doit :

– Utiliser les logiciels dans les conditions des licences souscrites.

– Ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages Web, textes, images, photographies, musiques, vidéos ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

– Respecter le droit des marques.

b) Respect du règlement général sur la protection des données personnelles

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement des données à caractère personnel, conformément au RGPD et à la loi n°78-17 du 6 janvier 1978 dite « Informatiques et Libertés » modifiée.

Ces dispositions s'appliquent à toute création de fichiers comprenant des informations à caractère personnel et aux demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants.

La communication de données à caractère personnel doit être sécurisée, c'est-à-dire que la confidentialité, l'intégrité et l'authenticité des informations doivent être assurées.

c) Respect de la vie privée

Le droit à la vie privée, le droit à l'image et le droit de représentation impliquent qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne sans un consentement de la personne intéressée.

d) Respect des clauses contractuelles

Les ressources documentaires électroniques éditoriales dans les conditions contractuelles des licences souscrites par l'établissement : usage raisonnable (pas de téléchargement de livres complets ou de fascicules entiers de revues, pas d'utilisation d'aspirateur de site Web), usage personnel et strictement non commercial (interdiction de distribuer des copies papier ou de diffuser des versions numériques à toute personne extérieure à l'établissement, même à titre gratuit).

e) Responsabilité en matière de transmission d'informations

L'utilisateur devra entre autres s'abstenir :

– De diffuser des messages diffamatoires ou injurieux (ces faits sont répréhensibles, quel que soit leur mode de diffusion, public ou privé).

– D'utiliser certaines formes d'apologie (crime, racisme, négationnisme, crimes de guerre …).

– D'utiliser toute forme de provocation et de haine raciale ; de diffuser des informations confidentielles sans autorisation préalable d'une personne habilitée.

ARTICLE III. PRINCIPES DE SÉCURITÉ

Section III.1 Règles de sécurité applicables

L'EFA met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.

En particulier tout utilisateur du système d'information de l'EFA doit être référencé dans les bases de référence de l'établissement et avoir obtenu des codes d'accès «authentifiant et mot de passe», qui lui sont personnels et confidentiels.

Une politique de sécurisation des mots de passe a été instaurée à l'EFA suivant les recommandations de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité permettant de protéger les données et les outils auxquels il a accès de toute utilisation malveillante ou abusive. Cette mesure ne confère pas pour autant un caractère personnel à ces données ou outils.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée. La sécurité des systèmes d'information mis à sa disposition lui impose :

– De respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe.

– De garder strictement confidentiel son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers.

– De respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à les connaître.

– De protéger son certificat électronique (s'il en dispose) par un mot de passe sûr gardé secret.

Comme la signature manuscrite, le certificat électronique est strictement personnel et l'utilisateur s'engage à n'autoriser personne à en faire usage à sa place.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe, il devrait procéder, dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur. Le bénéficiaire de la communication du mot de passe ne peut le communiquer à son tour à un tiers ni l'utiliser en dehors de la circonstance exceptionnelle qui lui a fait bénéficier de ce mot de passe.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

a) de la part de l'EFA :

– Veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service misent en place par la hiérarchie.

– Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

– Ne pas autoriser les redirections de messagerie pour les adresses électroniques de fonctions dans la mesure ou le système d'information est accessible (après authentification) tant du réseau de l'établissement que de l'extérieur.

b) de la part de l'utilisateur :

– S'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information et aux communications entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite.

– Ne pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des données et informations confidentielles ou contraires à la législation en vigueur.

– Ne pas connecter directement aux réseaux filaires des matériels autres que ceux confiés ou autorisés par l'EFA. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée.

– Ne pas connecter au réseau wifi nommé EFA-WIFI des matériels autres que ceux confiés ou autorisés par l'EFA. Un réseau EFA-INVITES est dédié à la connexion de matériels de toute provenance, ainsi le matériel personnel peut se connecter à ce réseau dans le respect de la charte informatique.

– Ne pas installer, télécharger ou utiliser sur le matériel connecté au réseau de l'EFA, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation du service informatique ou de sa hiérarchie.

– Ne pas déposer des données sur un serveur interne ou ouvert au grand public ou sur le poste de travail d'un autre utilisateur sans y être autorisé par les responsables habilités.

– Ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites (virus, chevaux de Troie, bombes logiques…). Tout travail de recherche ou autre, risquant de conduire à la violation de cette règle, ne pourra être accompli qu'avec l'autorisation du responsable de la sécurité du système d'information (RSSI) de l'établissement et dans le strict respect des règles qui auront alors été définies.

– Se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques.

– Assurer la protection de ses informations et plus particulièrement celles considérées comme sensibles. En particulier, il ne doit pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports non fiables tels que les ordinateurs portables, clés USB, disques externes, etc.

– Ne pas quitter son poste de travail ni ceux en libre-service en laissant des ressources ou services accessibles.

– Alerter au plus tôt de tout dysfonctionnement ou risque de sécurité en contactant le service informatique ou son supérieur hiérarchique.

Section III.2 Devoirs de signalement et d'information

L'EFA doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information.

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, etc.

Il signale également au Responsable de la sécurité des systèmes d'information (RSSI) toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation.

Section III.3 Mesures de contrôle de la sécurité

L'utilisateur est informé :

– Que pour effectuer la maintenance corrective, curative ou évolutive, l'EFA se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition.

– Qu'une maintenance à distance est précédée d'une information de l'utilisateur.

– Que toute information bloquante ou présentant une difficulté technique d'acheminement à son destinataire peut être isolée, le cas échéant supprimée.

L'EFA informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Les personnels en charge des opérations de contrôle sont soumis au secret professionnel. Ils ne peuvent donc pas divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction dès lors que :

– Ces informations sont couvertes par le secret des correspondances ou, identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.

– Elles ne mettent en cause ni le bon fonctionnement technique des applications ni leur sécurité.

– Elles ne tombent pas dans le champ de l'article 40 alinéa 2 du code de procédure pénale française qui fait obligation à tout organe public de déférer des faits délictueux au procureur de la République.

ARTICLE IV. COMMUNICATIONS ÉLECTRONIQUES

Section IV.1 Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'EFA.

La messagerie est un outil de travail ouvert à des usages professionnels (administration, pédagogie, recherche) ; elle peut constituer le support d'une communication privée telle que définie à l'article II. À cette fin, l'établissement recommande fortement l'utilisation d'adresses électroniques privées.

a) Adresses électroniques

Une adresse électronique nominative est attribuée à chaque utilisateur qui la gère sous sa responsabilité. Sa forme est standardisée prenom.nom@efa.gr

L'utilisation d'une adresse électronique, fonctionnelle ou organisationnelle, est fortement conseillée pour un utilisateur ou un groupe d'utilisateurs.

b) Contenu des messages électroniques

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place.

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé. Dans ce cas et afin de lui conserver son caractère privé, l'utilisateur doit le déposer dans un dossier identifiable comme « personnel ».

c) Émission et réception des messages

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

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles [6] 1369-1 à 1369-11 du Code civil.

Les utilisateurs doivent en conséquence, être vigilant sur la nature des messages électroniques qu'ils échangent au même titre que pour les courriers traditionnels.

e) Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou utiles en tant qu'éléments de preuve.

À ce titre, il doit notamment se conformer aux règles définies dans la présente charte et, le cas échéant, dans le ou les guides d'utilisation établi(s) par le service ou par l'établissement.

Section IV.2 Internet

Il est rappelé que l'Internet est soumis à l'ensemble des règles de droit en vigueur.

a) Publications sur les sites Internet de l'EFA

Toute publication de pages d'informations ou de documents sur les sites Internet, plateformes applicatives de l'institution ou réseaux sociaux de l'EFA doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication de pages d'information (ou documents) à caractère privé sur les ressources du système d'information de l'institution n'est autorisée, sauf disposition particulière.

Il est à noter que les pages, dites personnelles professionnelles :

– Sont des pages Web du domaine « efa.gr » (ou d'un de ses sous-domaines) placées sous la responsabilité d'un personnel de l'établissement, d'une association, d'un groupement ; elles doivent être fiables et l'on doit pouvoir facilement les dater, identifier leur producteur et comprendre à quel titre il les rend accessibles.

– Contiennent des informations de nature professionnelle, en rapport avec le métier du responsable ou avec les missions de l'EFA ce qui implique une responsabilité sur le contenu informatif (exactitude, légalité, pertinence, ...), leur pérennité et leur intégrité.

– Concourent comme les autres à l'image de l'établissement et des autres tutelles dans le cas des unités mixtes de recherche; il est donc interdit d'engager l'établissement et les autres tutelles ou de nuire à leur réputation ou à celle de l'un de leurs membres.

b) Sécurité

L'EFA se réserve le droit, à tout moment, de filtrer ou d'interdire l'accès à certains sites, ports réseaux, applications et de procéder au contrôle a priori ou a posteriori des communications créées ainsi que des durées d'accès correspondantes.

Ces accès ne sont autorisés qu'au travers des dispositifs de sécurité mis en place par l'EFA. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'établissement.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de campagnes de sensibilisation.

c) Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur le réseau Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VI. L'EFA se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'EFA, code malicieux, programmes-espions ...).

À l'inverse, l'utilisation du réseau pour l'offre d'un service disponible depuis l'Internet doit être rationnelle de manière à éviter toute consommation abusive. L'offre de sons, d'images, de vidéos, de logiciels et tous autres documents doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis dans la section II.3 et être en rapport avec les missions d'enseignement et de recherche de l'EFA.

ARTICLE V. TRAÇABILITÉ

L'EFA est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées.

L'EFA a mis en place des outils de traçabilité sur les différents systèmes d'information.

Un document décrivant la politique de gestion des journaux informatiques (et mentionnant notamment la durée de conservation des traces) à usage interne du service informatique a été créé.

ARTICLE VI. LIMITATIONS DES USAGES

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation, le directeur de l'établissement pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire. Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles, est passible de sanctions.

Engagement de confidentialité des systèmes d'information

Définition des informations confidentielles

Ce sont tous les documents, fichiers, informations, qu'ils soient informatisés ou manuscrits relatifs au système d'information de l'École française d'Athènes qui ne sont pas rendus publics.

En particulier cela concerne le réseau de l'établissement, ses serveurs et applications, son environnement de sécurité informatique (fichiers de configuration, mots de passe, données nominatives, fichiers journaux), les messages électroniques.

Engagement

Je soussigné(e) _____, m'engage à respecter la confidentialité des informations auxquelles j'aurai accès dans l'exercice de mes fonctions ou des missions qui me sont confiées, sauf autorisation explicite de l'établissement, et ceci pour une durée indéterminée.

Je reconnais avoir pris connaissance de la charte des utilisateurs concernant l'usage du système d'information de l'EFA et m'engage à la respecter.

Plus particulièrement, je m'engage :

1. à n'accéder qu'aux renseignements nécessaires à l'exécution de mes tâches ;
2. à n'utiliser ces renseignements que dans le cadre de mes fonctions ;
3. à ne révéler aucun renseignement concernant les données confidentielles dont j'aurai pris connaissance dans l'exercice de mes fonctions, à moins d'y être dûment autorisé ;
4. à n'intégrer ces renseignements que dans les seuls dossiers prévus pour l'accomplissement des mandats qui me sont confiés ;
5. à conserver ces dossiers de sorte que seules les personnes autorisées puissent y avoir accès ;
6. à protéger par un mot de passe, l'accès à l'information confidentielle que je détiens ou à laquelle j'ai accès ;
7. à informer sans délai le Responsable des Sécurité des Systèmes d'Information (RSSI) de l'établissement de toute situation ou irrégularité qui pourrait compromettre de quelque façon que ce soit, la sécurité, l'intégrité ou la confidentialité des informations.

Date :

Signature :