**Délibération du conseil académique du 22 juin 2023**

**N°CAC-23-0622-04**

# Charte informatique et numérique

## Le conseil académique de l'Université Gustave Eiffel

**Vu** le décret n°2019-1360 du 13 décembre 2019 portant création de l'Université Gustave Eiffel et approbation de ses statuts et notamment l'article 9.2 ;

**Vu** la charte informatique et numérique et la présentation jointes à la présente délibération.

**Considérant que** *depuis sa création l'Université Gustave Eiffel déploie progressivement un système d'information unique, il était nécessaire de pouvoir proposer une charte commune aux agents et étudiants en substitution aux chartes existantes de l'ESIEE Paris, l'ex-IFSTTAR et l'ex-UPEM ;*

**Considérant que** *la charte informatique et numérique est une annexe du règlement intérieur de l'Université Gustave Eiffel ;*

**Considérant que** *le conseil académique émet un avis sur les modifications du règlement intérieur ;*

**Considérant qu***'il est demandé au conseil académique de donner un avis sur le projet de charte informatique et numérique, tel qu'il lui a été présenté, lors de la séance.*

## Délibère

### Article 1er

**Après en avoir délibéré, le conseil académique émet un avis favorable sur la Charte informatique et numérique, à la majorité comme suit :**

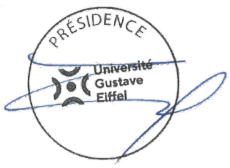
| | | |
|---|---|---|
| **Nombre de votants** | **:** | **54** |
| **Nombre d'abstentions** | **:** | **8** |
| **Nombre de votes pour** | **:** | **43** |
| **Nombre de votes contre** | **:** | **3** |

### Article 2

Le président de l'Université Gustave Eiffel est chargé de l'exécution de la présente délibération.

**Le président de l'Université Gustave Eiffel**
À Champs-sur-Marne, le 28 juin 2023

**Gilles ROUSSEL**



# Charte de bon usage des moyens informatiques et numériques de l'université Gustave Eiffel

**PROJET**

## Statut du document

Le comité social d'administration (CSA) a examiné les dispositions de la version 1.0 de cette charte lors de sa séance du XX/XX/20XX.

Sa date d'entrée en vigueur est fixée au XX/XX/20XX, date à laquelle elle a fait l'objet d'une communication à l'ensemble des agents en poste. Elle est une annexe du règlement intérieur.

Elle sera réputée connue des nouveaux personnels, auxquels elle sera remise lors de leur arrivée en poste, en tant qu'annexe au règlement intérieur. La charte sera librement consultable sur le système d'information de l'Université Gustave Eiffel accessible à l'ensemble des utilisateurs qu'elle concerne.

## Préambule

L'Université Gustave Eiffel met à disposition des utilisateurs autorisés un système d'information nécessaire à l'exercice des missions de service public de l'enseignement supérieur et de la recherche. La présente charte a pour objet d'encadrer les modalités d'usage du système d'information et l'utilisation des outils informatiques et numériques au sein de l'établissement, en précisant :
• d'une part, les moyens mis en œuvre par l'administration, garante du respect de la législation et de la réglementation en vigueur et de la sécurité des systèmes d'information ;
• d'autre part, les règles que doivent respecter les utilisateurs des outils informatiques et numériques mis à leur disposition.

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et numériques de l'Université Gustave Eiffel visant à préserver le système d'information. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes de disponibilité, d'intégrité, de confidentialité et de traçabilité des informations traitées.
Les usages des ressources informatiques et numériques non conformes aux préconisations de la présente charte peuvent être regardés comme des fautes susceptibles d'entraîner pour l'utilisateur une suspension conservatoire des outils mis à disposition, des sanctions disciplinaires, sans préjudice d'éventuelles 'actions pénales ou civiles à son encontre.

La charte est diffusée à l'ensemble des utilisateurs par tout moyen et à chaque modification. À ce titre, une version informatique de celle-ci est mise à disposition sur le site internet de l'Université. Elle est systématiquement communiquée à tout nouvel arrivant.
Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

## Article 1 : Définitions

***Utilisateur :***

Toute personne / individu ayant accès ou utilisant les moyens informatiques et numériques de l'Université Gustave Eiffel ou qui traite des données de l'Université Gustave Eiffel, quel que soit son statut et quel que soit son lieu d'exercice ou son mode de travail (sur site, en télétravail…). Il s'agit de :

- tout agent titulaire ou contractuel concourant à l'exécution des missions de service public de l'université ;
- tout étudiant inscrit ou en cours d'inscription pour l'année en cours, ou ayant été inscrit à l'université ;
- tout stagiaire utilisant ou ayant accès aux moyens informatiques et numériques de l'université ;
- tout lecteur autorisé qui dispose d'un accès aux ressources bibliographiques en ligne ;
- tout prestataire sous contrat avec l'Université ;
- tout personnel « hébergé » dans le cadre de conventions ;
- toute personne accueillie temporairement au sein de l'Université et ayant de ce fait accès à un poste informatique et/ou au réseau informatique (conférencier, chercheur invité, visiteur etc.).

***La direction de l'informatique et du numérique désigne l'unité de l'****Université Gustave Eiffel* en charge de ses ressources informatiques et numériques.

***Les moyens informatiques et numériques de l'Université Gustave Eiffel*** comprennent :

- les équipements informatiques, les serveurs, les postes de travail, les équipements mobiles (téléphone, tablette, portable, …) ainsi que leurs périphériques ;

- les réseaux locaux et longues distance connectés directement ou indirectement aux équipements de l'Université Gustave Eiffel ;
- les logiciels installés sur ces matériels ;

Certains moyens informatiques peuvent être sous-traités à des prestataires.
Dans ce qui suit, on désignera collectivement ces moyens par le terme de "système d'information".

***Système d'information (SI)*** : ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications mis à disposition par l'université.

***Données concernées*** :

Sont concernées, les données traitées par notre système d'information, y compris sur les matériels mobiles (PC, clef USB, ...) qu'il s'agisse des données de la recherche, de la formation, administratives (RH, comptabilité), ou transitant sur un dispositif d'information de l'Université Gustave Eiffel (mail, échange de fichiers, ...). Sont comprises les données qui sortent de notre système d'information, qu'elles soient hébergées sur un autre système, ou sur un matériel mobile hors des locaux de l'Université Gustave Eiffel.
Ressources numériques concernées :
- Les services numériques internes ou externes ;
- Les ressources documentaires ;
- Les sites web internes ou externes.

***Usages concernés*** :

La présente charte s'applique à tous les types d'usage de moyens et de ressources informatiques et numériques, quelle que soit leur fréquence ou leur périodicité et qu'ils aient lieu :
- dans les locaux de l'établissement, quelle que soit leur localisation ;
- dans le cadre d'un usage « nomade » quel qu'en soit le lieu ;
- dans le cadre d'un accès distant, quel que soit le lieu de cet accès.

***Information professionnelle*** : information utilisée en contexte de travail. Sa sensibilité est qualifiée selon quatre critères (publique, interne, confidentielle, secrète).

***Traitements de données*** : opérations informatisées ou pas portant sur des données telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

***Donnée à caractère personnel*** : toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
Une personne est identifiée lorsque son nom apparaît dans un fichier. Une personne est identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification : adresses postales et électroniques (courriel) ; IP (identification de la machine utilisée) ; numéro d'immatriculation ou de compte bancaire, identifiants de connexion, numéro de téléphone, numéro de sécurité sociale ; photographie ; voix ; données de localisation…
Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès la ou le responsable du traitement ou toute autre personne. Une donnée à caractère personnel peut donc aussi être une donnée professionnelle.

***Délégué à la protection des données (DPD-DPO)*** : personne chargée de la protection des données au sein de l'université.

***L'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI)*** est la personne responsable juridiquement, pour sa structure, de la sécurité des systèmes d'information. Il s'agit du président de l'université.

***Responsable de la sécurité du système d'information (RSSI)*** : personne chargée de la sécurité du système d'information. Elle est nommée par le président de l'université.

## Article 2: Portée, opposabilité et champ d'application

La présente charte s'applique à toute personne, dénommée « utilisateur » dans la suite du document, à qui l'usage d'un ou plusieurs outils informatiques et numériques est consenti par l'Université. Étant annexée au règlement intérieur, elle est applicable de fait et produit, à ce titre, les mêmes effets.
En conséquence, chaque utilisateur est supposé en avoir pris connaissance et doit l'appliquer.

Ces règles s'appliquent aussi implicitement aux personnes extérieures, notamment lorsqu'elles utilisent les services « invités » ou « visiteurs » (par exemple wifi), sous la responsabilité d'un agent de l'Université Gustave Eiffel organisateur de la réunion ou du contact dans l'université de l'organisateur d'une réunion.

Il est de la responsabilité de ces personnes extérieures d'avoir un matériel adapté, compatible et correctement configuré avec le système d'information de l'Université Gustave Eiffel pour un bon fonctionnement des services fournis par l'Université Gustave Eiffel.

L'usage des outils informatiques et numériques par les organisations syndicales fera l'objet d'une décision spécifiques[1] après avis du comité social d'administration.

Les prescriptions de cette charte pourront être précisées ou complétées ultérieurement en tant que de besoin, notamment en fonction des évolutions législatives et réglementaires et feront l'objet de publication adéquate.

## Article 3 : Engagements

**Engagements de l'université**

L'université doit veiller à la disponibilité, l'intégrité et la confidentialité de ses données et de son système d'information.

En ce sens elle en définit les règles d'usage qu'elle porte à la connaissance de l'utilisateur par la présente charte.
L'université met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.
L'université facilite l'accès des utilisateurs aux ressources du système d'information dont l'usage est nécessaire à l'exercice de leurs fonctions. Les ressources mises à leur disposition sont principalement à usage professionnel.

**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, de discrétion 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.
En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

[1] Arrêté du 4 novembre 2014 relatif aux conditions générales d'utilisation par les organisations syndicales des technologies de l'information et de la communication dans la fonction publique de l'Etat

## Article 4 : Dispositions législatives et réglementaires applicables

Chaque Utilisateur est tenu de respecter l'ensemble du cadre légal et règlementaire lié à l'utilisation du système d'information ainsi que toute autre règlementation susceptible de s'appliquer. A ce titre, il peut voir sa responsabilité individuelle engagée du fait d'une mauvaise utilisation. Le présent article a pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires définissant les droits et les obligations des personnes utilisant les moyens informatiques et numériques. Il ne s'agit en aucun cas d'une liste exhaustive.

**- Le Code Pénal, notamment ses articles 323-1 à 323-7 relatifs à la fraude informatique.**

**- Le Code de la propriété intellectuelle**

Il est strictement interdit à l'utilisateur d'utiliser, de reproduire et plus généralement d'exploiter des œuvres protégées par tout droit de propriété intellectuelle, notamment le droit d'auteur sans l'autorisation de l'auteur ou du titulaire des droits, particulièrement des documents textes, des images, de la musique, de la vidéo, y compris des œuvres qui seraient la propriété de l'université conformément à la législation en vigueur.

Les logiciels rentrent dans la catégorie d'œuvre de l'esprit et, à ce titre, le code de la propriété intellectuelle les protège sans nécessité de dépôt ou d'enregistrement**.**

**- Le Code général de la fonction publique,** notamment le livre 1er, titre II, chapitre 1er portant dispositions relatives aux obligations de réserve, de discrétion et de secret professionnel des agents publics et le titre I chapitre III relatif au droit syndical.

**- La loi n°78-17 du 6 janvier 1978 modifiée**, relative à l'informatique, aux fichiers et aux libertés, qui a notamment pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'emploi de l'informatique et d'encadrer l'utilisation des données à caractère personnel dans les traitements informatiques.

**- La loi n°94-665 du 4 août 1994 modifiée,** relative à l'emploi de la langue française.

**- Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril, dit Règlement Général sur la Protection des Données (RGPD)** qui constitue le texte de référence en matière de protection des données à caractère personnel.

**Télétravail**

**-** Article 133 de la loi n° 2012-347 du 12 mars 2012 modifiée a consacré la possibilité pour les agents publics (fonctionnaires ou non) d'exercer leurs fonctions dans le cadre du télétravail.

- Décret n°2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique.

**Réseaux sociaux**

- Déclaration des droits de l'homme et du citoyen de 1789

- Code pénal : Article R621-1

- Loi du 29 juillet 1881 modifiée relative à la liberté de la presse (art. 32 et 33)

## Article 5 : Conditions d'accès et d'utilisation du système d'information

### 5.1 Droits d'accès au système d'information à un usage professionnel

Le droit d'accès au système d'information est temporaire, personnel et incessible. Il est attribué individuellement à l'utilisateur normalement enregistré auprès du responsable informatique du site ou Campus selon la procédure d'ouverture d'un compte nominatif en vigueur dans l'université.

Ce droit d'accès est accordé exclusivement pour les activités professionnelles et/ou universitaires des utilisateurs. Il disparaît en cas de départ de l'utilisateur de l'université : lorsque le contrat ou l'activité est terminé, ou si le comportement de l'utilisateur est contraire aux règles énoncées par la présente charte.
Lors de l'ouverture du compte, l'utilisateur reçoit un ou plusieurs identifiants de connexion qui peuvent lui donner accès, en relation avec les besoins de son activité :

- à au moins un poste de travail, dédié ou partagé ;
- à une adresse de messagerie professionnelle pour les personnels et les étudiants de l'Université, ou une redirection, ou à une adresse étudiante ;
- au réseau interne ;
- aux serveurs de l'université et aux services et applications qu'ils hébergent ;
- à l'internet et aux ressources numériques de l'université.

### 5..2 Usage vie privée résiduelle des ressources informatiques et numériques

Un usage privé est toléré à condition qu'il soit raisonnable, licite et qu'il n'affecte pas la sécurité et le fonctionnement normal des services.
Par défaut, les usages et contenus sont réputés professionnels ; seuls les espaces, répertoires, fichiers et/ou messages qualifiés expressément de « personnels » ou de « privés » seront considérés comme tels.
En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel. Sous réserve de règles particulières de confidentialité, les collègues de travail ou les supérieurs hiérarchiques pourront avoir accès à ces derniers, en particulier pour assurer la continuité de service en cas d'absence prolongée en application des procédures en vigueur.

Dans tous les cas, y compris pour un usage privé, l'utilisation doit être conforme à l'ordre public et aux bonnes mœurs et ne doit pas mettre en cause ou porter atteinte à l'intégrité, à la réputation ou à l'image de l'administration (par exemple sont proscrits la consultation de sites ou de contenus de nature pornographique, terroriste, de jeux...).

L'usage privé des ressources informatiques et numériques peut être restreint par l'Université, notamment, dans un souci de bon usage des ressources (sécurité, performance...).

### 5. 3. Règles d'utilisation des ressources informatiques et numériques

Les utilisateurs sont responsables, en tout lieu, de l'usage qu'ils font du système d'information de l'Université Gustave Eiffel. Ils sont tenus à une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels elles et ils accèdent.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles

Les utilisateurs utiliseront uniquement les identifiants personnels. En cas de besoin, ils pourront demander des identifiants supplémentaires, le partage d'identifiant, même temporairement, n'est pas autorisé.
Par ailleurs, les utilisateurs encadrant des stagiaires peuvent en tant que de besoin leur faire ouvrir des comptes nominatifs. Les comptes génériques anonymes ne sont pas autorisés sauf exception en conformité avec les procédures en vigueur.

L'utilisateur protégera son compte par la technologie fournie (mot de passe, certificat, badges, ...). L'utilisateur devra respecter les règles de sécurité préconisées par l'université concernant le choix des mots de passe ainsi que des modalités d'utilisation des méthodes d'authentification.
Les utilisateurs occasionnels, comme les invités ou visiteurs utilisant les dispositifs qui leurs sont dédiés, comme le réseau Wi-Fi « invité », sont tenus de ne divulguer aucune information, comme les identifiants ou les configurations techniques, concernant le système informatique de l'Université Gustave Eiffel.

L'utilisateur est averti des nombreuses tentatives d'escroquerie visant à lui subtiliser ses identifiants (hameçonnage). Aussi il ne devra jamais communiquer ses identifiants, mots de passe, certificats, etc.…, en particulier en réponse à des courriers électroniques, suspects ou non, ou à des demandes téléphoniques. Il prendra les mesures préconisées par l'université pour en éviter une communication involontaire.
Si, par exemple pour un dépannage, il aurait besoin de communiquer un mot de passe ou un identifiant, ceci se fera de préférence en présence physique de la personne, dans tous les cas celle-ci devra être parfaitement identifiée, par exemple par une confirmation visuelle ou téléphonique.

En cas d'usage inapproprié au regard de la présente charte, l'utilisateur peut se voir suspendre ou retirer tout ou partie des moyens informatiques et numériques mis à sa disposition et peut se voir restreindre ses droits d'accès au système. Il pourra également faire l'objet d'une procédure disciplinaire.

L'utilisation des moyens informatiques et numériques de l'Université ou simplement de l'adresse de messagerie, respecte le principe de neutralité du service public et le devoir de réserve et de discrétion professionnelle.

### 5.4 Respect de la vie en collectivité et de consommation des ressources

L'utilisateur ne doit à aucun moment oublier qu'il vit et travaille au sein d'une communauté. Il s'interdit toute utilisation abusive d'une ressource commune (imprimante, réseau, espace disque, processeur, accès Internet, licences flottantes, etc.…) et veille à faire un usage sobre et raisonné des ressources. Les activités risquant d'accaparer fortement les ressources informatiques (impression de gros documents, calculs importants, utilisation intensive du réseau comme par exemple la consultation de contenu audio ou vidéo en temps réel, le téléchargement de fichiers nombreux ou volumineux, etc.) devront être effectuées sur les équipements dédiés à ces activités et selon les règles d'exploitation en vigueur ou aux moments qui pénalisent le moins la communauté et en accord suivant les situations avec les responsables ad hoc de la direction de l'informatique et du numérique qu'ils soient de proximité ou en central. En cas de doute, l'utilisateur pourra s'informer auprès de la direction de l'informatique et du numérique. En cas d'abus, la direction de l'informatique et du numérique pourra prendre des mesures visant à rétablir une utilisation plus équitable de ces ressources.

L'utilisateur s'exprimant au travers des moyens informatiques mis à sa disposition, en particulier sur des supports externes, devra le faire avec le respect du devoir de réserve et des règles de savoir vivre, son expression engageant directement ou indirectement l'Université Gustave Eiffel.

Les responsables de la direction de l'informatique et du numérique territoriaux ou centraux se réservent le droit de bloquer, en conformité avec les dispositions législatives et réglementaires et de la jurisprudence, l'accès à des sites ou à des services n'ayant aucun rapport avec l'exercice professionnel ou perturbant le bon fonctionnement du système.

L'utilisateur s'interdit de perturber volontairement tout autre utilisateur du système informatique, de masquer sa véritable identité[2] ou de s'approprier le mot de passe d'un autre utilisateur.

## Article 6 : Accès aux données et confidentialité

[2] Sauf dans des contextes définis comme l'usage de listes professionnelles fonctionnelles

## 6.1. Protection des données professionnelles

L'accès aux informations conservées ou circulant dans le système d'information doit être limité à ses propres données et aux données publiques. En particulier, il est interdit de copier, de prendre connaissance ou d'intercepter des informations détenues ou échangées par d'autres utilisateurs, sans leur autorisation, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux échanges du type messagerie électronique ou conversation directe, dont l'utilisateur n'est destinataire ni directement, ni en copie.

Les données professionnelles, en particulier les données du système d'information, les données expérimentales, les rapports, les logiciels, les résultats de calcul, etc. seront considérées comme bénéficiant d'un classement « Confidentiel université ».
A l'exception des données explicitement classées comme publiques et des échanges de données scientifiques dans le cadre de contrats prévoyant ces échanges avec les clauses de confidentialité correspondantes, ces données ne devront faire l'objet d'aucune communication ou stockage extérieur, sauf autorisation expresse du RSSI ou de l'AQSSI de l'Université Gustave Eiffel.

## 6.2 Protection des données personnelles

Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel, prévues pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » en vigueur et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018.
Dans ce cadre, les utilisateurs devront informer le Délégué à la protection des données et se conformer à la procédure en vigueur pour la mise en œuvre d'un traitement de données à caractère personnel.

Conformément à la législation applicable à la protection des données personnelles, les principes directeurs à respecter dans le cadre de la mise en œuvre d'un traitement de données personnelles sont les suivants :

- le respect des finalités initiales du traitement ;
- la pertinence et l'exactitude des données au regard des finalités poursuivies ;
- l'information des personnes à la collecte des données et la conservation du recueil de leur consentement en cas de signature électronique ou manuscrite ;
- le droit d'accès, de rectification ;
- le droit d'opposition ;
- la mise en œuvre de mesures de sécurité adaptées à la sensibilité des données traitées, résultant d'une étude d'impact pour les personnes privées en cas de divulgation, altération ou destruction des données les concernant.
- le contrôle rigoureux de la diffusion de données à caractère personnel à l'attention de tiers extérieurs, en incluant notamment les clauses adaptées dans les contrats avec les sous-traitants.
- la destruction des données au-delà de la période de conservation prévue.

Par conséquent, tout utilisateur est tenu d'assurer la protection des données à caractère personnel qu'il traite dans le cadre de ses fonctions notamment en :

- limitant strictement aux besoins de son activité la diffusion par des moyens informatiques ou autre (impressions papier par exemple) des données à caractère personnel en sa possession ;
- protégeant les codes d'accès aux applications et systèmes d'information qu'il utilise ;
- ne conservant pas ces données au-delà de la durée nécessaire au traitement auquel elles sont destinées ;
- informant immédiatement sa hiérarchie, ou la déléguée à la protection des données, ou le responsable de la sécurité du système d'information le cas échéant, si toute personne utilisatrice des outils informatiques, services numériques et des moyens de communication constatait un défaut dans la protection de données à caractère personnel ;

- sécurisant la communication de données à caractère personnel, afin que la confidentialité, l'intégrité et l'authenticité des informations soient assurées.
- impliquant la déléguée à la protection des données pour tout projet de transmission interne ou externe de données.

Tout traitement de données à caractère personnel, y compris la simple collecte, doit être analysé, étudié et répertorié dans le registre des traitements.

Lors de la réforme du matériel de stockage informatique (disques dur, clef USB, bande de sauvegarde, …) les données stockées devront être détruites de manière sûre (destruction physique des supports, démagnétisation, …) suivant les préconisations en vigueur.

## Article 7- Sécurité du système d'information

### – 7.1 Préservation de l'intégrité des informations

L'utilisateur s'engage à ne pas modifier ou détruire d'autres fichiers ou flots d'information que ceux qui lui appartiennent en propre, sauf accord de leur propriétaire. En particulier, il lui est interdit de modifier les informations contenues dans les journaux du système auxquels il aurait accès.

Si l'utilisateur est amené à constituer et/ou remplir des fiches, journaux, cahiers de laboratoires correspondant à des données relatives à des équipements ou logiciels appartenant à l'Université Gustave Eiffel, le responsable de ces traitements devra veiller à ce que la traçabilité des informations recueillies soit assurée par l'archivage dans le laboratoire ou unité correspondante.

L'utilisateur a la responsabilité d'archivage public des documents qu'il possède, selon la définition donnée par l'article L 211-4 du code du patrimoine.

Il est rappelé que les données de travail appartiennent à l'employeur, l'utilisateur doit être attentif à les protéger et ne pas les divulguer sans le consentement explicite de l'employeur. En particulier en cas d'export de ces données à l'extérieur, l'utilisateur doit examiner avec précaution les contrats d'hébergement, surtout gratuits, pour ne pas céder les données à des tiers non consentis (cas de la plupart des fournisseurs de volumes de stockages gratuits). Dans tous les cas l'utilisateur devra avoir le consentement du RSSI de l'Université Gustave Eiffel.

De même, l'attention de l'utilisateur est attirée sur les données à caractère personnel (au sens du RGPD), et notamment le numéro de sécurité sociale (NIR) et les données dites sensibles (informations concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle) où des précautions particulières doivent être prises. Dans le doute, la direction de l'informatique et du numérique pour les aspects techniques et/ou le service des affaires juridiques pour les aspects réglementaires, peuvent être consultés.

La direction de l'informatique et du numérique de l'université exploite différents systèmes de sauvegarde des données des utilisateurs, dans le cadre d'un engagement de moyens. L'utilisateur ne pourra en conséquence se prévaloir d'un quelconque dommage en cas de destruction accidentelle de ses données.

**A son départ de l'université, l'utilisateur transférera ses données professionnelles à ses collègues concernés en accord avec son responsable et fera son affaire de l'archivage et de l'effacement de ses données personnelles.** L'utilisateur ne pourra se prévaloir d'un quelconque dommage en cas d'usage ultérieur ou d'effacement de ses données professionnelles ou en cas d'accès à ses données personnelles ou d'effacement de celles-ci.

## 7.2 Préservation de l'intégrité du système informatique

**L'utilisateur est responsable de l'utilisation qu'il fait de son poste de travail.**

**L'utilisateur s'engage à 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 connus sous le nom générique de virus, chevaux de Troie, bombes logiques... La direction de l'informatique et du numérique se réserve le droit de désinstaller tout logiciel perturbant le bon fonctionnement du poste de travail.

Il doit suivre les consignes de sécurité applicables au sein de l'université, notamment en matière d'accès et d'anti-virus.
L'utilisateur s'engage à ne pas désactiver les logiciels installés par la direction de l'informatique et du numérique concernant notamment la mise à jour de l'anti-virus, les mises à jour de sécurité du système d'exploitation, l'outil de gestion du parc, les outils de sauvegarde automatique, les outils de supervision.

La direction de l'informatique et du numérique ne demandera jamais la transmission des identifiants de connexion de l'utilisateur.

Il est rappelé que les administrateurs peuvent accéder aux postes de travail et données des utilisateurs (pour des besoins de diagnostic, de sécurité, d'installation de correctif, etc.), y compris à distance et en l'absence de l'utilisateur (ex. : mises à jour ou installation de correctifs la nuit, suppression de fichier infecté – y compris si celui-ci est de nature privée). Conformément à la législation en vigueur, il est rappelé que les administrateurs n'ont pas le droit de surveiller l'activité de l'utilisateur.
Il est rappelé que les administrateurs sont aussi autorisés à effectuer des vérifications des moyens d'authentification sur les ressources de l'université, afin de tester régulièrement, par exemple, la robustesse des mots de passe choisis par les utilisateurs, et ainsi les inciter à en améliorer la sécurité.

**L'utilisateur ne doit pas s'absenter de son bureau en laissant libre accès à son poste de travail**. **Il ne doit jamais quitter un poste de travail en libre-service sans se déconnecter.**

Si un utilisateur est amené à se servir du système d'information de l'Université Gustave Eiffel depuis l'extérieur, il ne peut le faire qu'en se conformant strictement aux procédures et en utilisant exclusivement l'outillage ad hoc mis à sa disposition. Il doit respecter les dispositions de la présente charte et appliquer les recommandations de la direction de l'informatique et du numérique de l'université. Il est porté à l'attention de l'utilisateur que lors de l'utilisation du tunnel VPN de connexion au système informatique de l'Université Gustave Eiffel, les flux réseau, en particulier la navigation sur internet, passeront par cette connexion, qu'ils soient ou non à destination du réseau de l'Université Gustave Eiffel.

La même vigilance doit s'appliquer s'il le fait à partir d'un micro-ordinateur portable de l'université, tout particulièrement si ce micro-ordinateur est utilisé pour se connecter au système informatique d'autres structures ou à des systèmes publics (Hot spot Wi-Fi par exemple).

La connexion au réseau informatique de nouvelles machines (postes de travail, périphériques, imprimantes, photocopieuses, dispositifs de visioconférence), le déplacement et/ou la modification de la connexion de machines existantes, la déconnexion de machines réformées, l'ajout de commutateurs, de bornes wifi, de modems ou de services aux réseaux, ne pourront être faits que sous la responsabilité de la direction de l'informatique et du numérique par application des procédures en vigueur, soit au niveau central ou au niveau local. Un contrôle est opéré par la direction de l'informatique et du numérique de l'université sur la connexion de nouveaux équipements.

Si l'utilisateur utilise un micro-ordinateur portable comme poste de travail, il doit se connecter régulièrement au réseau de l'université pour s'assurer de la bonne mise à jour de la solution antivirus et de l'application des correctifs de sécurité. Tout micro-ordinateur portable qui se connecterait rarement au réseau pourra être considéré comme un équipement neuf et soumis aux vérifications correspondantes.

Les postes de travail, fixes ou portables, doivent être redémarrés régulièrement, en particulier après l'installation de correctifs de sécurité.

L'installation de nouveaux logiciels, ou la modification de logiciels existants, ayant un impact sur des programmes ou des bibliothèques utilisées par la communauté des usagers d'un campus voire au-delà, ne pourra être faite que par le responsable informatique territorial ou central ou son représentant habilité.

Le transfert de données via un support externe (clef USB, disque externe, ...) depuis un poste de travail hors de contrôle de l'université, peut amener à une contamination par un virus. Cette opération devra se faire avec prudence, par exemple avec une analyse préalable du support externe par l'antivirus du poste destinataire. En cas de doute, contacter le représentant de la direction de l'informatique et du numérique de son lieu de travail.

L'utilisateur est informé de la présence de systèmes automatiques de filtrage, aussi bien sur le réseau que sur les serveurs et postes de travail. Ces dispositifs, comme les anti-virus, visent à maintenir en sécurité le système d'information. Occasionnellement ils peuvent filtrer des données légitimes, l'université ne pourra en être tenu responsable. Dans ce cas, une information sera délivrée pour éveiller la vigilance des utilisateurs.

## Article 8 : Traçabilité

L'utilisateur est informé que différents dispositifs du système informatique, liés aux obligations légales, à la gestion de la sécurité et de la qualité de service et à la recherche des pannes et incidents, enregistrent des événements le concernant.
Par conséquent des outils de traçabilité sont mis en place sur tous les systèmes d'information.

Ces enregistrements, qui n'ont pas par nature vocation à être des outils de surveillance individuelle, peuvent donner lieu à des analyses systématiques de volumétrie ou de détection de comportements anormaux. Ils peuvent à l'occasion être utilisés pour identifier des utilisations manifestement abusives au sens des différentes clauses de cette charte. Certains de ces outils peuvent être situés sur les postes de travail individuels.

L'utilisateur est informé que les mécanismes de sauvegarde peuvent garder trace d'activités le concernant ou de fichiers qu'il a par ailleurs décidé de supprimer, et ce pendant la durée de rétention maximale des différents supports de sauvegarde.

## Article 9 : Anomalies, analyse et contrôle de l'utilisation des ressources, droits d'administration

### 9.1 : Anomalies

Dans le cas :

- •d'anomalie pouvant mettre en cause la sécurité du poste, des données ou du système informatique,
- •de compromission ou de risque de compromission de son compte informatique,
- •de vol ou de perte de son ordinateur portable ou d'un autre support (téléphone, clef USB, ...) contenant des données de connexions aux ressources de l'Université Gustave Eiffel,

l'utilisateur préviendra immédiatement et en parallèle son supérieur hiérarchique et le responsable informatique identifié en pareil cas de la direction de l'informatique et du numérique, charge à lui d'alerter ou pas en fonction

de la situation le RSSI et/ou la DPO. Ce responsable prendra les mesures de protection nécessaires immédiates contre des menaces éventuelles.

En cas de vol, ceci ne décharge pas l'utilisateur des démarches administratives (par exemple, la déclaration de vol ...).

Lorsque des anomalies mettant en cause le bon fonctionnement ou la sécurité du système d'information sont relevées, ou lorsqu'elles révèlent une méconnaissance des droits de la propriété intellectuelle, ces anomalies sont signifiées à l'utilisateur par les voies appropriées et sont éliminées avec son accord. En cas de désaccord, le problème est remonté au niveau du responsable dont dépend l'utilisateur et à la direction de l'informatique et du numérique de l'université. En cas d'urgence, la direction de l'informatique et du numérique de l'université peut se passer d'un accord préalable.

De même, lorsque des faits susceptibles d'être pénalement sanctionnés sont constatés, le représentant de la direction de l'informatique et du numérique de l'université en informe la présidence et la direction générale des services de l'université qui prendront toutes les mesures nécessaires, y compris le porter à connaissance du Procureur de la République en conformité avec les obligations du fonctionnaire.

## 9.2 Maintenance, analyse et contrôle

Pour des nécessités de maintenance et de gestion technique, de contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus, l'utilisation des ressources informatiques et des services internet, ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de le législation applicable et notamment de la loi sur l'informatique et des libertés.

L'utilisateur dont le poste fait l'objet d'une maintenance à distance doit être préalablement informé.
Les personnels en charge des opérations de contrôle sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, en particulier lorsqu'elles sont couvertes par les secrets des correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service.

## 9.3 : Responsabilités et droits d'administration

L'administration des postes de travail est de la responsabilité de la direction de l'informatique et du numérique et des correspondants informatiques d'unité quand ils existent. Dans le cas où un utilisateur dispose des droits d'administration de son poste de travail, il est tenu :

- de réserver l'utilisation de la connexion comme administrateur aux tâches qui le nécessitent et de travailler habituellement avec un profil simple utilisateur ;
- de se conformer aux consignes d'administration énoncées par la direction de l'informatique et du numérique ;
- d'appliquer les dispositions de la présente charte ;
- de respecter les contrats signés avec les fournisseurs de logiciels, ainsi que leurs closes particulières concernant les étudiants ou les personnels, en particulier en matière de copie et d'usage.

## Article 10 - Limitation des usages et sanctions

L'utilisateur est tenu de respecter l'ensemble des règles définies dans la présente charte, ainsi que les textes de référence applicables rappelés dans le présent document.

Tout manquement à ces règles et mesures de sécurité et de confidentialité est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des sanctions disciplinaires et pénales en fonction de la gravité des faits constatés par les instances compétentes. L'université via la direction de l'informatique et du numérique se réserve le droit de restreindre ou de suspendre sans préavis son accès au système d'information ou son accès à l'Internet, de lui supprimer les droits d'administrateur de son poste de travail, d'installer sur son poste de travail un logiciel de supervision et de prendre toute autre mesure qu'il jugera nécessaire.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est également passible de sanctions.

Il est rappelé que l'université peut être amenée, en réponse à la demande d'une autorité judiciaire, à fournir au requérant les mots de passe, l'adresse IP interne (et le nom de l'utilisateur de ladite adresse IP à l'horodate donnée) à l'origine d'une connexion vers l'Internet ou toute autre donnée qui intéresserait le requérant pour les besoins de son enquête.

Je soussigné(e) : .....

certifie avoir pris connaissance des règles de bonne conduite énoncées dans la présente charte informatique et numérique de l'Université Gustave Eiffel et m'engage à m'y conformer strictement.

A ..... le .....

(Signature à faire précéder de la mention manuscrite « lu et approuvé »)

.....

## Annexe 1

## Textes de référence en matière informatique (au 31/12/2022)

I- LES TEXTES LEGISLATIFS ET REGLEMENTAIRES

La loi du 29 juillet 1881 modifiée sur les infractions de presse

Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

Loi n° 83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires (article 26)

La loi n° 84-16 du 11 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique de l'Etat (1), et notamment l'article 15 de la loi n° 84-16 du 11 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique de l'Etat

La loi Godfrain du 5 janvier 1988, relative à la fraude informatique, est la première loi française réprimant les actes de criminalité informatique et de piratage.

La loi n°91-646 du 10 juillet 1991 modifiée relative au secret des correspondances émises par la voie des communications électroniques et son rectificatif

La loi n° 94-665 du 4 août 1994 modifiée relative à l'emploi de la langue française.

La directive européenne 97 / 66 du 15 décembre 1997 qui s'applique aux courriers postaux et aux courriers électroniques.

Loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique.

Ordonnance n° 2005-1516 du 8 décembre 2005 modifiée relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Décret n° 2011-184 du 15 février 2011 modifié relatif aux comités techniques dans les administrations et les établissements publics de l'Etat et notamment son article 34 :
« Les comités techniques sont consultés, dans les conditions et les limites précisées pour chaque catégorie de comité par les articles 35 et 36 sur les questions et projets de textes relatifs :
(…) 4° Aux évolutions technologiques et de méthodes de travail des administrations, établissements ou services et à leur incidence sur les personnels ; ».

La directive NIS (Directive Network and Information Security) publiée en 2013 par la Commission.

Circulaire du Premier ministre N°5725/SG du 17 juillet 2014 relative à la Politique de sécurité des systèmes d'information.

Instruction interministérielle n°901 relative à la protection des systèmes d'informations sensibles (publiée le 11/02/2015).

Décret 2022-513 du 8 avril 2022

Instruction générale interministérielle IGI-1337 du 26 octobre 2022.

Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (cloud computing) - référentiel d'exigences Version 1.3 du 30/07/2014.

Chartes d'utilisation de la Fédération Éducation-Recherche (RENATER).

II_ LES CODES

CODE DE LA FONCTION PUBLIQUE

https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000044416551/2022-03-01

CODE PENAL ET CODE DE PROCEDURE PENALE

Les articles 226-16 à 226-24 du Code pénal définissent et prévoient les sanctions applicables dans les cas d'atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques.

Les articles 323-1 et suivants du Code pénal visent à lutter contre la fraude informatique en réprimant :
- Les accès ou maintien frauduleux dans un système d'information,
- Les atteintes volontaires au fonctionnement,
- La falsification des documents informatiques et leur usage illicite,
- L'association ou l'entente en vue de commettre un de ces délits.

Un paragraphe du Code pénal définit et prévoit les sanctions en cas d'atteinte au secret de la correspondance (Article 226-15).
Le Code pénal définit et prévoit les sanctions applicables en cas de vol, recel, destructions, dégradations et détériorations de biens dans son livre III « Des crimes et délits contre les biens ».
Le Code pénal définit ce qui présente un caractère de secret de la défense nationale et y associe des sanctions.
L'article 40 du Code de procédure pénal prévoit l'obligation pour tout fonctionnaire de signaler tout crime ou délit dont il aurait connaissance au Procureur de la République.

Les articles 227-22 et suivants du Code pénal prévoient les sanctions dans les cas d'atteinte aux droits des mineurs, de crimes ou délits envers les mineurs (notamment pédopornographie) au moyen d'un réseau de communications électroniques.

LE CODE CIVIL

Article 9 : respect de la vie privée

Article 1366
L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Article 1240
Celui qui causerait à un autre un dommage serait tenu de le réparer.

Article1241:
Chacun reste responsable du dommage qu'il a causé non seulement par son fait, mais encore, par sa négligence ou par son imprudence

LE CODE DE LA PROPRIETE INTELLECTUELLE
https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414

CODE DES POSTES ET DES COMMUNICATIONS ELECTRONIQUES

Article L34-1 et suivants

- .

## ~~Annexe 2~~

***~~Dispositions spécifiques à une catégorie d'utilisateurs (ex. Étudiants)~~***

~~A compléter~~

## Annexe ~~3~~2

***Dispositions spécifiques ~~à une catégorie d'utilisateurs~~ : cours de réseau et de cybersécurité***

**~~Utilisation de laboratoires spécifiques et clubs de l'université Gustave Eiffel~~**

~~La direction de l'informatique et du numérique peut mettre à disposition des enseignants et étudiants des laboratoires spécifiques pour des cours de réseau ou de cybersécurité. Lors de ces cours, les étudiants sont connectés avec des droits d'administrateur sur les ordinateurs.~~
~~L'accès à ces laboratoires ne sera autorisé pour ces étudiants qu'une fois qu'ils auront signé la décharge de responsabilité juridique valable pour une année scolaire et donnée en annexe 2 de ce document. Les enseignants utilisant ces laboratoires s'engagent implicitement en signant cette présente charte à respecter les règles de cette décharge.~~

~~Les associations et clubs de personnels ou d'élèves doivent connecter les machines qu'ils utilisent dans le cadre de leur association sur le réseau dédié. Le président de l'association ou du club en charge de l'organisation d'une manifestation doit aussi signer la charte donnée en annexe 4.~~

Dans le cadre de ses activités pédagogiques, l'Université Gustave Eiffel peut être amenée à déroger à certains principes classiques d'une Politique de Sécurité des Systèmes d'Information (PSSI). Cette annexe a pour but de spécifier les exceptions autorisées pour les cours de réseau et de cyber-sécurité.

Authentification des utilisateurs :

Pour les cours de réseau et de cyber-sécurité, il est nécessaire de permettre aux utilisateurs de se connecter aux postes de travail avec un compte local générique avec des droits d'administrateur. Cette exception est autorisée dans la mesure où l'authentification des utilisateurs est effectuée lors de l'accès à Internet via un portail captif. Cette méthode permet de garantir la sécurité des systèmes d'information de l'université tout en permettant aux étudiants d'accéder aux ressources nécessaires pour les cours de cyber-sécurité.

Utilisation de logiciels et outils de sécurité :

L'université Gustave Eiffel peut être amenée à utiliser des logiciels et des outils de sécurité qui dérogent aux principes généraux d'une politique de sécurité. Cette exception est autorisée dans la mesure où ces logiciels et outils sont utilisés exclusivement à des fins pédagogiques et sous la supervision d'un enseignant qualifié en matière de sécurité informatique.

## Annexe 34 ~~:~~

**a mis en forme :** Police :14 pt

**a mis en forme :** Centré

### Décharge de responsabilité pour les clubs et associations étudiantes~~Information concernant les enseignements en réseau et cybersécurité~~

**a mis en forme :** Police :11 pt

**L'université Gustave Eiffel peut mettre à disposition de ses clubs et associations étudiantes une infrastructure informatique pour faciliter leurs activités. Cette infrastructure comprend des postes de travail, des serveurs, des réseaux et des outils de communication. Cependant, l'utilisation de cette infrastructure peut entraîner des risques pour la sécurité des systèmes d'information de l'université, ainsi que pour la confidentialité et l'intégrité des données.**

**Pour protéger les systèmes d'information et les données des utilisateurs, il est nécessaire que les responsables des clubs et associations étudiantes prennent des mesures de sécurité appropriées et respectent les règles et procédures établies en matière de sécurité informatique. Afin de formaliser cet engagement, l'Université Gustave Eiffel demande aux responsables des clubs et associations étudiantes de signer une décharge de responsabilité avant d'utiliser l'infrastructure informatique de l'université. Cette décharge de responsabilité a pour but de clarifier les responsabilités des parties impliquées et de garantir la sécurité des systèmes d'information.**

Je soussigné(e) : ……..
(cocher la case adaptée)

- Etudiant(e) à **Université Gustave Eiffel** pour le cours ou la filière : ……
- Président ou membre du club / de l'association : ……..

durant l'année scolaire 20….. - 20…..

Je déclare avoir pris connaissance du texte suivant, extrait de la loi relative à la fraude informatique : "L'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 de deux ans d'emprisonnement, et de 60 000€ d'amende".

Je suis également informé que la simple tentative est passible de la même peine.

Je m'engage sur l'honneur à ne jamais utiliser ou tenter d'utiliser les informations que j'aurais pu recevoir à **l'université Gustave Eiffel** dans un autre but ~~que celui de l'étude théorique en vue d'améliorer~~qui serait de nature à nuire à la sécurisation des systèmes d'information.

Fait le …… à ……..

Signature :

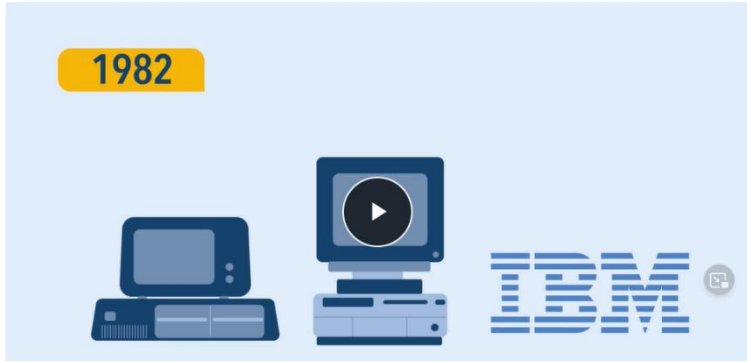
22 06 2023

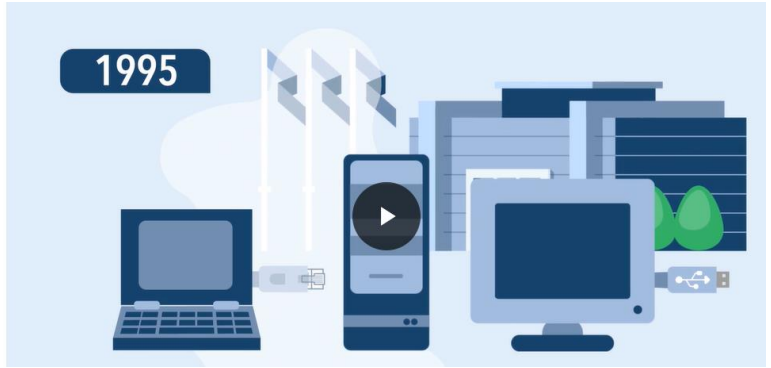
Mizzi Jean-Paul

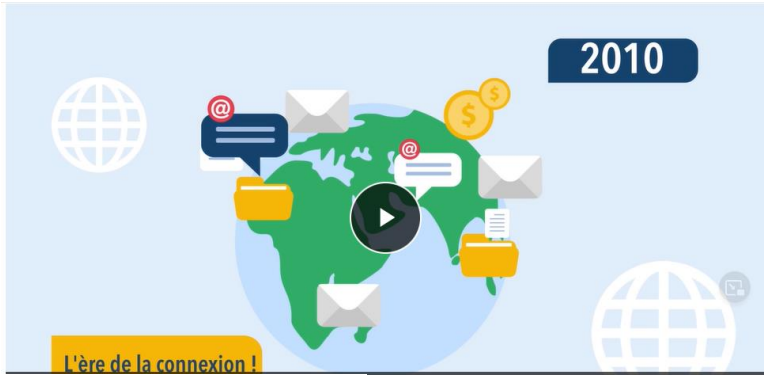
# Sécurité des Systèmes d'Information
# Charte de bon usage des moyens informatiques et numériques de l'Université Gustave Eiffel
# Cac 22 juin 2023

Université Gustave Eiffel

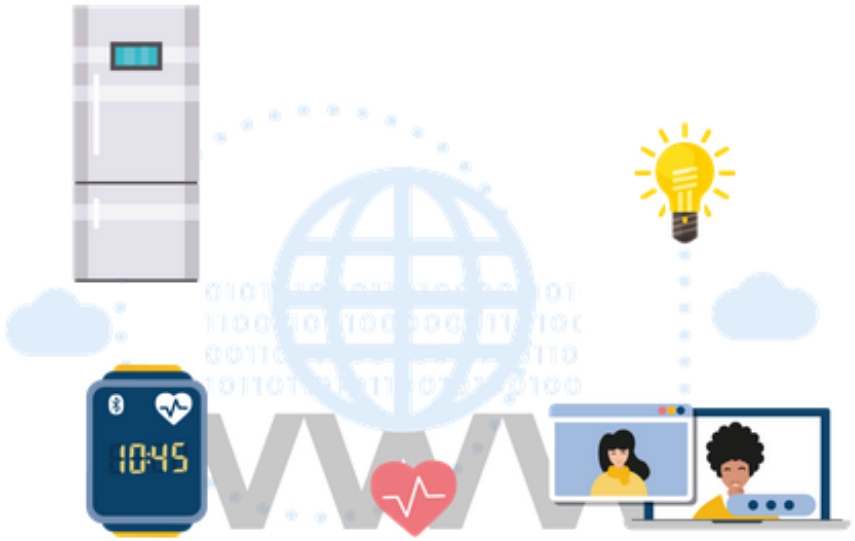
# Un monde hyperconnecté




Aujourd'hui, la diversité des objets connectés dans notre quotidien ne cesse de croître : des réfrigérateurs aux ampoules, **tout est accessible via Internet** depuis un ordinateur ou un ordiphone.




## Le cloud

**mutualisation** des **ressources de calcul et de stockage**

distribuées dans des **datacenters** répartis dans le monde entier.

Une activité non sans risque car risque de piratage et de non respect de la confidentialité

# L’ESR est aussi touché que les autres

Le nombre d’**attaques** cyber est en **augmentation notable** ces dernières années **(+37 %** entre 2020 et 2021) et l’ANSSI considère que 15 % d’entre elles ciblent le milieu éducatif et toujours **plus diverses et avancées**.
Une incidentologie très chargée, particulièrement au S2-2022 pour l’ESR.
Des exfiltrations de données tous les jours, par des approches basée sur de l’ingénierie sociale de plus en plus sophistiquées :

- 90% des attaques – réseaux sociaux utilisés comme base de données, habitudes de navigation
- 60% des IoT vulnérables par absence de privacy by design.
- 20% des attaques résultent de méthodes d’authentification compromises – collusion de Mot de passe entre privé et professionnel.

**Qu’est ce qui motive un cybercriminel : Faisabilité et Rentabilité**

**Notre bastion** – faire perte du temps à l’attaquant, le fatiguer, lui faire comprendre que nous attaquer va être difficile. Les clés du château sont les utilisateurs.

# L’ESR est aussi touché que les autres

Pour faire face à ces menaces, le cadre réglementaire évolue par la publication de 2 textes en 2022 qui précisent les obligations pesant sur tous les établissements publics :

- **Décret 2022-513 du 8 avril 2022**,
- **Instruction générale interministérielle IGI-1337 du 26 octobre 2022**.

**Une sécurité des SI efficace requiert compréhension, vigilance et organisation.**

Il faut construire un plan de résilience – deux axes d’accompagnement : métier et utilisateur.

**La charte du bon usage du système d’information**, un des piliers de la politique de sécurité de notre système d’information pour avoir une **pleine conscience** et une **maîtrise du risque**.

**Par cette charte y voir plutôt des mesures pour protéger nos libertés que définir un carcan**.

Ses finalités aider à : Anticiper, Identifier, Alerter et Agir – comme tout marin qui se respecte il faut regarder l’horizon.
Ne jamais se reposer sur ses lauriers. *L’adversaire apprend aussi de ses échecs…*

# Une exigence réaffirmée par la règlementation : l'homologation des services

Développer une stratégie d'**homologation de sécurité** de nos SI sur la base d'une analyse des risques principaux associés aux missions et activités de l'établissement en vue de classer les SI en trois niveaux : critique / sensible / standard.

Puis réaliser les homologations de sécurité en priorisant sur les SI les plus critiques.

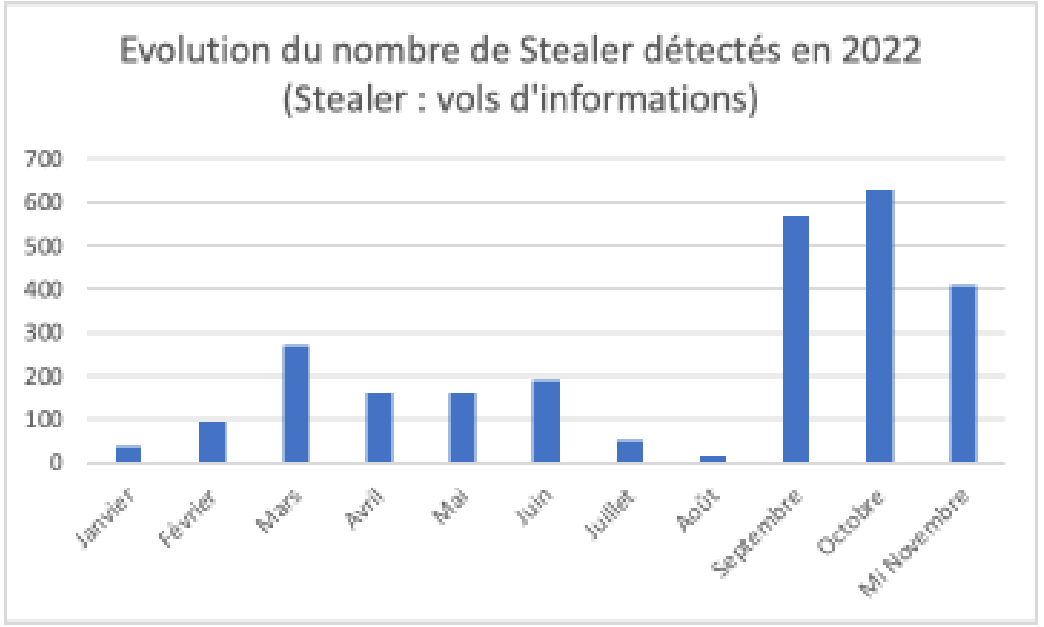
D'ici deux ans tous nos services en usage aujourd'hui doivent être homologués.

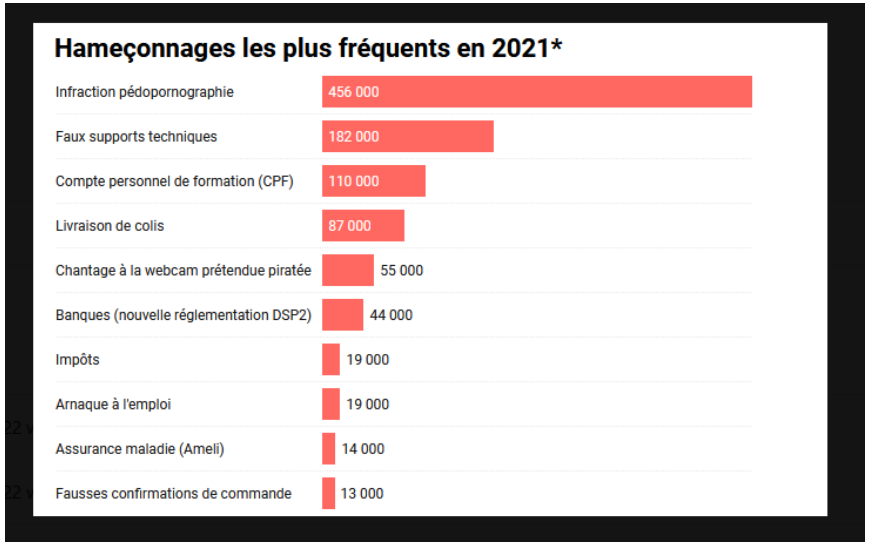
Tout nouveau service depuis octobre 2022, doit être homologué avant sa mise en exploitation.

Une commission d'homologation est en cours de création.

# Universités attaquées : de vrais impacts

- **Interruption des services** de plusieurs jours à plusieurs semaines (retour au papier-crayon)
- **Pertes financières** (dépenses et recettes)
- **Destruction de données** (parfois irrémédiable)
- **Vol de données** (agents, étudiants)
- **Perte de confiance**
- **Crise politique**
- **Crise sociale**
- **Mise en cause judiciaire** (individuelle ou collective)
- **Atteinte à la réputation**




Université Gustave Eiffel

# Des freins et préjugés au quotidien

Une fois spolié, ne pas se dire trop tard que l'on fera de la sécurité

Le Corbeau et le Renard
« La cybersécurité, je ne suis pas concerné ! »



Le Loup et l'Agneau
« La cybersécurité, ce n'est pas ma priorité ! »

Priorité forte – top 3. A trop repousser sa cybersécurité on finit en pleurs.

**Risque perçu faible et pas de clés pour l'éviter**
**Pourtant de vrais menaces**

La Cigale et la Fourmi
« La cybersécurité, je n'ai pas le budget ! »


Rien ne sert de reporter il faut se protéger maintenant

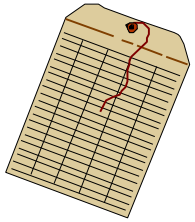
Le Lièvre et la Tortue
« La cybersécurité, je n'ai pas le temps »

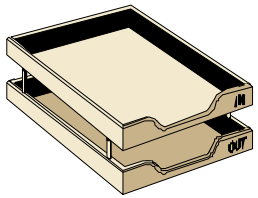

Budget SSI 7 à 10 % *par rapport au budget total d'un SI.*

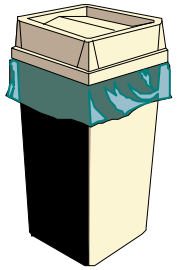
Université Gustave Eiffel

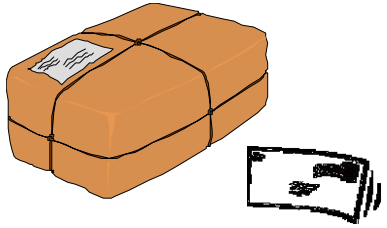
# Un système d'information c'est quoi?

Système d´information :
organisation des activités consistant
à acquérir, stocker, transformer, diffuser, exploiter, gérer
… les informations









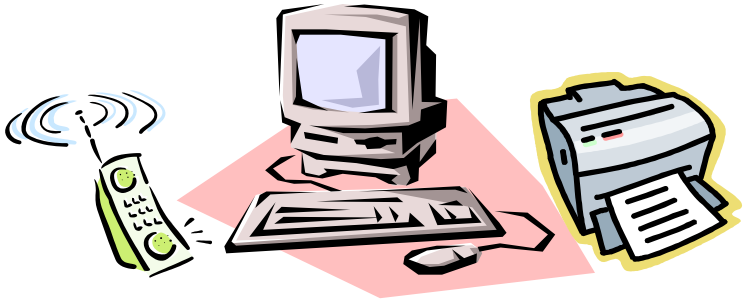
**Une « donnée »** est **une information** qui englobe plusieurs caractéristiques : un type, une criticité, des droits et des moyens d'accès.

**Une donnée** peut se présenter sous différents formats :

- physique (documents papiers, affiches, livres, etc.)

- numérique – fichiers (ppt, xls, doc, odt, odp, jpeg, html, sons, vidéos, animations, etc.)

**Un des moyens techniques**
pour faire fonctionner un système d'information est d'utiliser un Système informatique

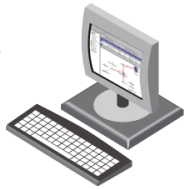


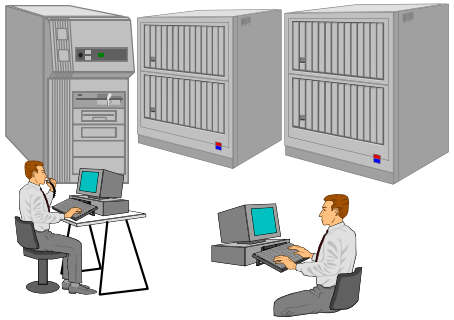
Les données sont ce que le cerveau est à l'être humain : **mémoire et intelligence**

Université Gustave Eiffel

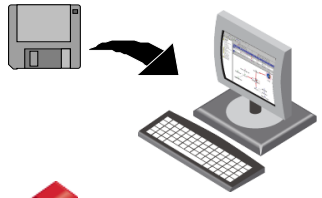
# La SSI c'est donc notamment :
## Assurer la sécurité des systèmes informatiques

Erreurs de saisie

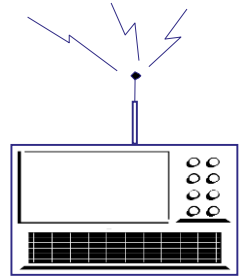




Virus



**L'intégrité des données**, c'est-à-dire sur la modification non-autorisée d'une donnée.

Attaques réseau

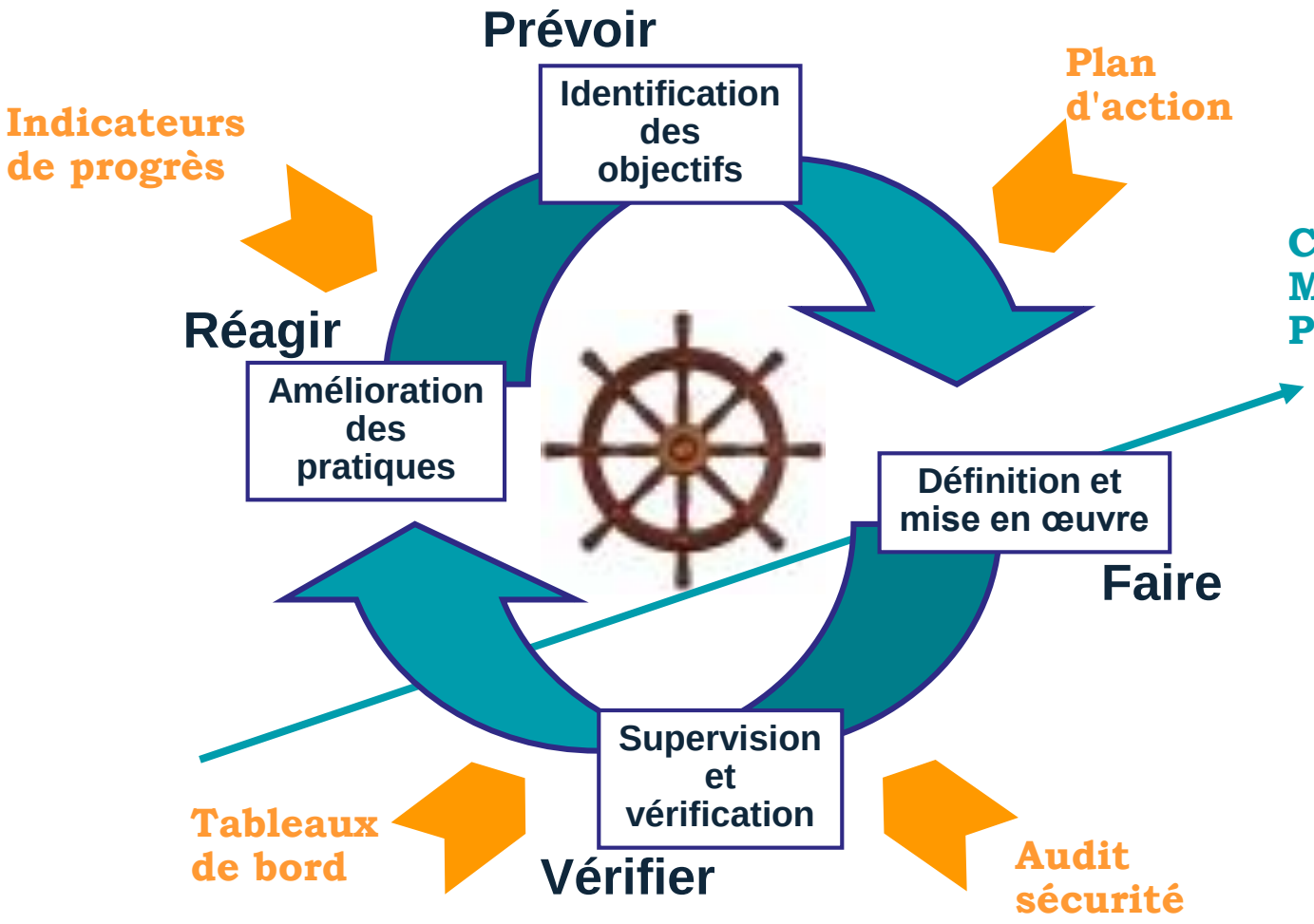
Accès illicites (intrusion)

Rayonnements

# L’organisation au sein de notre université

- **L’autorité qualifiée** (AQSSI) - le Président
- Un **comité de pilotage SSI et** un **comité opérationnel** pouvant basculer en cellule de crise
- Une équipe RSSI s’appuyant sur des **correspondants** dans les composantes, laboratoires et services de l’université, premier point d’entrée au plus proche des utilisateurs.
- Tous les personnels de la DGDIN pour la mise en œuvre et la gestion opérationnelle de la SSI. Ils sont également mobilisés pour la supervision des infrastructures et services ainsi que pour la remontée des alertes et la diffusion des bonnes pratiques.
- Une ligne directrice Zéro trust : Vérification continue, Privilège proportionné, Segmentation, Inspection des charges utiles, Analyse comportementale des flux pour détecter les activités suspectes.

# Une organisation s'appuyant sur une démarche d'amélioration continue




## 5S – Kaizen

| | |
|---|---|
| Seiri | Trier |
| Seiton | Arranger |
| Seiso | Nettoyer |
| Seiketsu | Standardiser |
| Shitsuke | Faire évoluer |

改善

*Roue de Deming ou PDCA (Plan / Do / Check / Act)*

# La Charte

Un engagement individuel pour un bien être collectif dans le but :

- **D'éviter les risques**
  - **sensibiliser : développer la prise de conscience et l'implication**
  - **prévenir : empêcher l'occurrence de l'événement**
  - **dissuader : prévoir des sanctions**

- **De faciliter la détection les attaques : déceler et identifier l'agression**

- **De limiter les dégâts**
  - **confinement : empêcher la propagation**
  - **riposte : mettre en place des mesures de sauvegarde, de destruction de l'information, des actions contre l'agresseur**
  - **réparation : annuler les conséquences et recouvrer la situation antérieure**

Pour finalement **augmenter la confiance**

# La Charte : C’est adopter les bonnes pratiques

**Etre attentif à :**

- **Ne pas contourner** les éléments de sécurité en place conformément à la charte et aux politiques de sécurité : antivirus, proxy, contrôle d’accès, droits, outils de chiffrement, redondance de sauvegarde, …

- **Respecter les consignes** de sécurité mises en place (non divulgation de mots de passe, classification des documents, usage des périphériques mobiles, n’emportez pas d’informations confidentielles afin d’éviter que celles-ci soient compromises, etc)

- **Respecter les règles d**e classement, de stockage ou de destruction des données édictées

- **Ëtre Vigilant au quotidien, alerter** : un ordinateur non verrouillé sans surveillance, un post it perdu qui semble contenir un pwd, des droits d’accès trop larges, un visiteur non accompagné
- **Réagir** : une attitude proactive pour éviter les incidents de sécurité, chaque seconde compte pour limiter les conséquences, corriger immédiatement une faille ou une anomalie par le signalement de l’incident permettra d’améliorer durablement la sécurité

# Charte de bon usage des moyens informatiques et numériques de l'université Gustave Eiffel - Sommaire

## Article 1 : Définitions

Toute personne ayant accès ou utilisant les moyens informatiques et numériques ou qui traite des données de l'Université, quel que soit son statut et quel que soit son lieu d'exercice ou son mode de travail (sur site, en télétravail…)

## Article 2 : Portée, opposabilité et champ d'application

La présente charte s'applique à toute personne, à qui l'usage d'un ou plusieurs outils informatiques et numériques est consenti par l'Université.
En conséquence, chaque utilisateur est supposé en avoir pris connaissance et doit l'appliquer.

## Article 3 : Engagements – université et utilisateur

L'université doit veiller à la disponibilité, l'intégrité et la confidentialité et la traçabilité de ses données et de son système d'information.
L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès.

## Article 4 : Dispositions législatives et réglementaires applicables

## Article 5 : Conditions d'accès et d'utilisation du système d'information : usage professionnel et personnel

Le droit d'accès au système d'information est temporaire, personnel et incessible. Il est attribué selon la procédure d'ouverture d'un compte nominatif en vigueur dans l'université.
Un usage privé est toléré à condition qu'il soit raisonnable, licite et qu'il n'affecte pas la sécurité et le fonctionnement normal des services.

Université Gustave Eiffel

# Charte de bon usage des moyens informatiques et numériques de l'université Gustave Eiffel - Sommaire

## Article 6 : Accès aux données et confidentialité

Les données professionnelles, les données expérimentales, les rapports, les logiciels, les résultats de calcul, etc. seront considérées comme bénéficiant d'un classement « Confidentiel université » sauf avis explicitement formulé.
Tout traitement de données à caractère personnel, y compris la simple collecte, doit être analysé, étudié et répertorié dans le registre des traitements.

## Article 7 : Sécurité du système d'information

A son départ de l'université, l'utilisateur transférera ses données professionnelles à ses collègues concernés en accord avec son responsable et fera son affaire de l'archivage et de l'effacement de ses données personnelles.
L'utilisateur ne doit pas laisser libre accès à son poste de travail. Il ne doit jamais quitter un poste de travail en libre-service sans se déconnecter.
Les postes de travail, fixes ou portables, doivent être redémarrés régulièrement, pour l'installation de correctifs de sécurité.

## Article 8 : Traçabilité

## Article 9 : Anomalies, analyse et contrôle de l'utilisation des ressources, droits d'administration

L'utilisateur préviendra immédiatement et en parallèle son supérieur hiérarchique et le responsable informatique identifié en pareil cas de la direction de l'informatique et du numérique, charge à lui d'alerter ou pas en fonction de la situation le RSSI et/ou la DPO.
L'administration des postes de travail est de la responsabilité de la direction de l'informatique et du numérique et des correspondants informatiques d'unité quand ils existent.

# Charte de bon usage des moyens informatiques et numériques de l'université Gustave Eiffel - Sommaire

## Article 10 : Limitation des usages et sanctions

L'utilisateur est tenu de respecter l'ensemble des règles définies dans la présente charte, ainsi que les textes de référence applicables rappelés dans le présent document.

Tout manquement à ces règles et mesures de sécurité et de confidentialité est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des sanctions disciplinaires et pénales en fonction de la gravité des faits constatés par les instances compétentes.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est également passible de sanctions.

## Vos contacts utiles


**Jean-Paul Mizzi - RSSI**

jean-paul.mizzi@univ-eiffel.fr

**Benjamin Dupalut – RSSI adjoint**

Benjamin.dupalut@univ-eiffel.fr

**Christian Jobic- RSSI adjoint**

Christian.jobic@univ-eiffel.fr

**Fabrice Lorrain- RSSI adjoint**

Fabrice.lorrain@univ-eiffel.fr


Université Gustave Eiffel