
		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020


CHARTE D'UTILISATION DES MOYENS INFORMATIQUES

LOUVRE

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

Sommaire

CHARTE D'UTILISATION DES MOYENS INFORMATIQUES	1
1 Objet et champ d'application	3
2 Définitions / Abréviations	3
Article 1 : Accès aux systèmes d'information	5
Article 2 : Gestion des mots de passe et codes d'accès.....	6
Article 3 : Verrouillage des postes de travail	6
Article 4 : Usage de la messagerie professionnelle.....	6
Article 5 : Utilisation des matériels et des espaces de stockage	7
Article 6 : Usage d'internet	10
Article 7 : Télétravail	10
Article 8 : Travail en mode nomade	11
Article 9 : Confidentialité	12
Article 10 : Propriété Intellectuelle.....	12
Article 11 : Obligations relatives aux données à caractère personnel.....	13
Article 12 : Protection de l'image de l'établissement.....	14
Article 13 : Droit à la déconnexion.....	14
Article 14 : Conditions d'un usage privé	15
Article 15 : Disposition en cas d'absence, de départ ou de décès d'un agent.....	17
Article 16 : Supervision des systèmes d'information.....	18
Article 17 : Respect de la Loi Informatique et liberté par l'établissement	19
Article 18 : Responsabilité et sanction.....	21
Article 19 : Entrée en vigueur	22

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

1 Objet et champ d'application

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques mis à la disposition du personnel du Musée du Louvre et ainsi :

- garantir le bon fonctionnement des Systèmes d'Information au service des missions du Musée du Louvre ;
- participer à la protection du patrimoine numérique du Musée du Louvre ;
- préserver la sécurité des systèmes d'information ;
- assurer la confidentialité des données ;
- limiter la prolifération erratique des logiciels ;
- éviter l'atteinte à des droits privés.

La sécurité des systèmes d'information n'est pas qu'une question technique portée par des spécialistes. C'est évidemment une condition nécessaire mais pas suffisante. Nous sommes tous acteurs à notre niveau de la cyber sécurité du Musée du Louvre de par notre attitude et notre vigilance. Chacun a un rôle primordial à jouer.

Les règles décrites dans la présente charte s'appliquent au personnel du Musée du Louvre qui utilisent les moyens informatiques de l'établissement ainsi que tout autre moyen de connexion à distance afin d'accéder, via le réseau informatique, à tout service de communication ou de traitement électronique interne ou externe, y compris l'accès à Internet.

Un document cadre complémentaire fixe les usages par les organisations syndicales du Musée du Louvre des technologies de l'information et de la communication mises à leur disposition par l'établissement. L'objectif de ce document cadre est de simplifier l'action quotidienne des acteurs du dialogue social, tout en veillant au respect de la liberté syndicale et à la préservation du bon fonctionnement de l'outil de travail, propriété du Musée du Louvre.

2 Définitions / Abréviations

Identification / Authentification :

La saisie du nom d'utilisateur permet l'identification.


La saisie du mot de passe permet l'authentification.

Ressources informatiques :

Ce sont les moyens matériels (ordinateurs, serveurs, imprimantes, téléphone, smartphones, ...) et logiciels mis à disposition des utilisateurs dans le cadre des fonctions occupées.

Systèmes d'Information :

Ensemble des éléments et règles participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l'information au sein de l'Établissement et vers ses partenaires externes.

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

Données à caractère personnel :

Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable. Une personne physique peut être identifiée notamment par référence à élément tel qu'un nom, des données de localisation (adresse), une photographie, un n° de téléphone, une adresse mail, ou un ou plusieurs éléments spécifiques propres à son identité physique, génétique, économique, culturel, social... ces données sont des données à caractère personnel.

Données à caractère personnel particulières :

Il s'agit de données sensibles qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le traitement de ces données est par principe interdit. Si de telles données devaient être recueillies, il convient de se rapprocher de la cellule RGPD (Cf. politique interne de la protection des données à caractère personnel).


Abréviations :

SDSI : Sous-Direction des Systèmes d'Information

RSSI : Responsable Sécurité des Systèmes d'Information

DPD : Délégué à la protection des données


ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

Article 1 : Accès aux systèmes d'information

L'autorisation d'accès est accordée par l'autorité hiérarchique compétente puis mise en place par la SDSI.

1. Cette autorisation se concrétise par l'ouverture d'un compte utilisateur et l'accès à l'un des postes de travail de l'établissement. A chaque utilisateur relié au réseau informatique interne est associé un compte, un mot de passe ainsi que la plupart du temps une adresse de messagerie électronique.
2. L'accès aux logiciels métiers de l'établissement est soumis à une autorisation spécifique en fonction du profil métier de l'agent. La demande exprimée par l'utilisateur doit être transmise par écrit aux référents métiers via les correspondants informatiques des départements/directions.
3. Ces autorisations d'accès sont strictement personnelles et confidentielles. Il est dès lors interdit à l'utilisateur de :
 - procéder à la moindre divulgation, même intra-service, de son ou de ses moyens d'authentification ;
 - de mettre à disposition, même temporairement, d'un tiers son ou ses moyens d'authentification ;
 - supprimer, masquer ou modifier son identité ou son identifiant ;
 - utiliser un moyen d'authentification autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;
 - user de son droit d'accès pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès ;
 - lorsqu'un accès distant lui est accordé, d'utiliser d'autres moyens d'authentification que ceux qui lui sont remis à cet effet.
4. Sauf à avoir engagé préalablement une demande de suspension ou de suppression d'autorisation, ou à être en mesure de démontrer le contraire, tout usage des moyens informatiques et outils numériques est réputé avoir été réalisé par le ou les bénéficiaires en cas de moyens d'authentification communs à plusieurs utilisateurs (comptes dits génériques), qui en assume toute conséquence, notamment juridique et financière.
5. Tout droit prend fin lors du départ de l'utilisateur, de la cessation de son activité professionnelle, ou en cas de non-respect des dispositions de la présente charte par l'utilisateur.
6. Lors de son départ, l'utilisateur restitue à la SDSI les matériels mis à sa disposition. Il doit préalablement effacer ses éventuels fichiers et données privés de son espace de stockage personnel et de sa messagerie. Toute copie de documents professionnels est interdite sans autorisation préalable du supérieur hiérarchique. L'utilisateur doit également archiver ses documents électroniques conformément à la politique d'archivage de l'établissement consultable sur le site intranet.

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

Article 2 : Gestion des mots de passe et codes d'accès

Les utilisateurs peuvent accéder aux systèmes d'information de l'établissement en utilisant un code d'accès et un mot de passe respectant les recommandations de la SDSI.

L'identifiant et le mot de passe sont strictement personnels et confidentiels, ils constituent une preuve de sa responsabilité quant à l'utilisation des moyens informatiques de l'Établissement. L'utilisateur s'engage donc à ne jamais le communiquer, ni à permettre à un tiers d'accéder à son compte.

S'il n'existe pas de processus automatique de renouvellement, l'utilisateur doit renouveler ce mot de passe personnellement tous les 6 mois.

Les mots de passe utilisés dans la sphère professionnelle ne doivent pas être réutilisés dans la sphère privée.

Ils s'engagent à signaler au RSSI toute tentative de violation de leur accès individuel au système d'information via l'ouverture d'un incident auprès de l'assistance informatique et une notification par mail à l'adresse ssi@louvre.fr.

Article 3 : Verrouillage des postes de travail

Qu'il s'agisse d'un poste fixe ou d'un portable, l'utilisateur ne doit pas quitter son poste de travail en laissant des ressources ou logiciels accessibles, même pour une courte durée.

En règle générale, l'utilisateur devra à minima verrouiller son poste de travail en cas d'absence de courte durée.

Suivant la durée de l'absence, une fermeture de la session est recommandée.

Pour des raisons de sécurité, écologiques et financières, l'extinction des ordinateurs est obligatoire à la fin de son service.


Article 4 : Usage de la messagerie professionnelle

La messagerie est réservée à un usage professionnel et engage la responsabilité de l'utilisateur au même titre que tout autre moyen de communication.

L'utilisateur doit faire preuve de mesure et de discrétion lorsqu'il s'exprime par l'intermédiaire des outils de communication. Il doit également s'abstenir de publier des messages contraires à l'ordre public, diffamatoires, racistes, xénophobes, homophobes, sexistes, injurieux, portant atteinte à la décence ou constituant une diffusion de fausses informations. Il doit prendre toutes dispositions pour consulter, reproduire ou transmettre de manière licite les données ou œuvres protégées par des droits d'auteur, sous quelque forme que ce soit.

Une utilisation privée occasionnelle et raisonnable est tolérée conformément à l'article 14 de la présente charte.

Il convient de faire régulièrement le tri et d'évaluer la pertinence de conserver ou non les messages, particulièrement ceux contenant des pièces jointes. La messagerie électronique n'est pas un espace de stockage.

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

Il est recommandé de ne pas divulguer son adresse électronique sur des forums ou sur des sites Internet non professionnels, en raison du risque de virus et de surcharge inutile de la boîte de messagerie (spam).

Ne sont, notamment, pas autorisées les pratiques suivantes :

- la diffusion d'un courriel ou document en grand nombre (spam), sauf utilisateurs spécifiques
- la diffusion collective démultipliée d'un message en cascade (principe de chaîne)
- l'inscription et l'usage des listes de diffusion autre que strictement professionnelles (en assurant au préalable et, de manière continue, de la pertinence et de la nécessité de celle-ci, ainsi que de ses conséquences (fréquence de réception des messages, poids des messages, encombrement des réseaux, notamment)
- rediriger manuellement ou automatiquement les mails reçus vers une messagerie personnelle.

Il est interdit d'utiliser l'adresse de messagerie professionnelle pour des usages personnels sur les réseaux sociaux ou autres services internet, sans rapport avec l'activité professionnelle.

Il convient de faire preuve d'une grande vigilance quant aux messages contenant des liens internet ou des pièces jointes et de signaler tout message suspect au RSSI via l'ouverture d'un incident auprès de l'assistance informatique et une notification par mail à l'adresse ssi@louvre.fr.

Article 5 : Utilisation des matériels et des espaces de stockage

L'établissement met à disposition de chaque utilisateur les équipements dotés des outils informatiques nécessaires à l'accomplissement de ses fonctions.

Tout utilisateur d'une ressource informatique mise à disposition par l'établissement doit prendre toutes les dispositions pour en éviter le vol ou la détérioration.


Ces matériels, de type PC fixe, PC portable, téléphone fixe, téléphone sans fil, smartphone, imprimante... sont fragiles et requièrent d'être manipulés de façon adaptée. Les utilisateurs sont sensibilisés aux bons usages des matériels et s'engagent à les manipuler en conséquence.

L'utilisateur ne doit pas déplacer, connecter ou déconnecter du réseau ces équipements sans y avoir été autorisé par la SDSI.

Toute action susceptible de mettre en cause la sécurité matérielle ou juridique de l'établissement, d'entraîner une baisse notable des performances globales des systèmes d'information ou de constituer une gêne, est interdite.

Poste de travail :

L'utilisateur s'interdit d'installer des programmes, des matériels ou autres outils informatiques sans l'accord de la SDSI. Le poste professionnel ne peut être utilisé que par l'agent ou parfois le service auquel il a été affecté, pour les finalités professionnelles définies.

			MDL
	Charte d'Utilisation des Moyens Informatiques		MDL - SSI
			1 - 0
			26/11/2020

Toute connexion sans autorisation de périphériques personnels (Disque Dur, Clé USB, Webcam...) à un poste de travail de l'établissement ou d'ordinateur personnel aux réseaux (Wi-Fi, filaire, ...) de l'établissement est interdite.

Périphériques USB :

Les périphériques de type clés USB ou disques durs externes doivent être utilisés à des fins professionnelles. Seul le matériel appartenant à l'établissement peut être connecté.

Imprimantes :

L'utilisateur est responsable du bon usage des imprimantes et responsable des données qu'il imprime. Il doit s'assurer de ne pas laisser à la vue de tous les documents sensibles imprimés.

Téléphonie fixe, smartphones et tablettes :

L'établissement met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles. Les smartphones et tablettes fournis par l'établissement sont à usage strictement professionnel.

Seuls ces périphériques peuvent être connectés aux réseaux dédiés sécurisés et accéder entre autre au systèmes de messagerie ou à des applications métiers spécifiques.

Des restrictions d'utilisation des téléphones fixes et mobiles (par exemple, certains postes sont limités aux appels nationaux) sont mises en place en tenant compte des missions de l'utilisateur.

L'utilisation voix des téléphones à titre privé est admise à condition qu'elle demeure raisonnable.

Les téléphones personnels et professionnels ne doivent en aucun cas être raccordés par prise USB au poste de travail de l'utilisateur. Les téléphones professionnels ne doivent être rechargés que directement sur des prises électriques.

Objets communicants :


En règle générale, aucun objet communicant (Montre connectée, Bracelet, lecteur de Carte à puce, capteur, etc.) ne peut être connecté aux réseaux (filaire, Wi-Fi, etc.) de l'établissement sans l'aval de la SDSI, qui aura procédé à toutes les vérifications nécessaires à la validation du dispositif.

Applications en ligne :

Les applications en lignes, téléchargées gratuitement ou achetées sur les stores (Google, Apple, Microsoft, etc.) ne peuvent être utilisées et intégrées aux processus métiers de l'établissement sans qualification préalable par la SDSI. L'usage de ce type d'application, sans assurance de respect des critères d'intégrité, de confidentialité, de disponibilité et de traçabilité, sans connaissance détaillée des conditions générales de vente ou d'usage, engage la responsabilité de l'utilisateur.

Stockage et partage de données en ligne (« dans le nuage / cloud ») :

L'utilisation de services gratuits, de type « Cloud grand public » offrant des possibilités de stockage temporaire en ligne (WeTransfer, Grosfichier, YouSendIt, etc.) ou de partage de données en ligne (DropBox, GoogleDrive, Onedrive, etc.) présente un risque pour l'établissement.

			MDL
	Charte d'Utilisation des Moyens Informatiques		MDL - SSI
			1 - 0
			26/11/2020

Ce type de « Cloud Computing » est une forme particulière d'utilisation de ressources informatiques "hors site" pour laquelle l'emplacement physique des données dans le nuage n'est pas porté à la connaissance des utilisateurs et cibles récurrentes de cyber attaques.

Cet usage ne répond donc pas au besoin de conformité légale indispensable à une administration publique en ne garantissant ni la territorialité, ni la disponibilité, ni l'intégrité, ni la confidentialité et ni la traçabilité des données stockées ou partagées.

L'envoi de documents en interne ou vers nos partenaires extérieurs est donc strictement interdit par ces services en ligne et il convient donc d'utiliser exclusivement les outils mis à disposition par l'établissement pour le partage de documents ou les outils externes validés par la SDSI.

Pour ce qui concerne la réception de documents de l'extérieur, il convient de rappeler à nos interlocuteurs (s'ils utilisent ces solutions cloud grand public) leur devoir de sécurisation des échanges (nous pouvons citer par exemple les fichiers protégés par mot de passe, durée limitée de la mise à disposition, traçabilité des accès, cryptages des données pour les données personnelles ou confidentielles).

Intégrité des informations :

L'utilisateur ne doit pas :

- modifier ou détruire d'autres informations que celles dont il est gestionnaire.
- faire disparaître, ni altérer les informations dont il est gestionnaire et dont la suppression ou la modification pourrait avoir des conséquences dommageables pour l'établissement.


Espaces de stockage :

L'utilisateur doit, dans la mesure du possible, maîtriser ses espaces de stockage (pas de doublons, organisation efficace et lisible). Il doit veiller à n'y stocker que des données ayant une valeur professionnelle. Une tolérance est acceptée en ce qui concerne les disques durs des ordinateurs, où l'utilisateur peut définir un espace personnel explicite (« PRIVE » « Privé » « privé » « Prive » « prive »), sous réserve que les fichiers stockés ne mettent en cause ni leur bon fonctionnement technique, ni leur sécurité, ni les intérêts de l'établissement.

Afin de ne pas saturer les espaces de stockage, il convient d'y faire régulièrement le tri et de réévaluer la pertinence des données conservées. L'utilisateur doit respecter les règles d'archivage des documents électroniques conformément à la politique d'archivage de l'établissement.

Enfin, il est rappelé que l'ensemble des documents professionnels doit être stocké sur les espaces réseau dédiés, sécurisés et sauvegardés, et non pas sur les disques durs des postes de travail, non sécurisés et non sauvegardés. L'établissement ne pourra être tenu responsable de perte d'informations non stockées correctement.

Aucune donnée liée à l'activité de l'établissement ne doit être stockée sur des équipements personnels.

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

Article 6 : Usage d'internet

Seuls les sites Internet présentant un lien direct avec l'activité professionnelle ont vocation à être consultés.

Le téléchargement de fichiers, de logiciels, de vidéos, d'images, de sons, ainsi que la visualisation en ligne de médias non liés à l'activité professionnelle sont interdits.

Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité à apporter la preuve, le cas échéant, du bon usage des moyens informatiques et outils numériques mis à la disposition des utilisateurs, l'établissement met en œuvre des outils de traçabilité, tels que des journaux de connexions de l'ensemble des moyens informatiques et outils numériques. Les traces informatiques sont conservées pour une durée d'un an.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

L'établissement autorise un usage personnel raisonnable d'Internet, durant les temps de pause.

Article 7 : Télétravail


Le travail hors des murs de l'établissement implique une très grande vigilance des utilisateurs et le respect de règles spécifiques afin de garantir la sécurité et la confidentialité des données et ressources de l'établissement et de ses agents.

Les principaux risques liés à cet usage sont :

- le vol ou la perte de l'équipement nomade mis à disposition par l'établissement et de ce fait la perte de données métiers contenues dans celui-ci ;
- l'interception de données ou identifiants ;
- la compromission au travers de sites internet.

Les postes nomades sont conçus de manière à pallier un certain nombre de risques mais il réside tout de même une part de responsabilité du télétravailleur pour garantir la sécurité et l'intégrité de ces solutions :

- L'ordinateur est à usage strictement professionnel et ne doit pas être mis à disposition d'un tiers ;
- Prendre soin que l'environnement immédiat soit propice au respect de la confidentialité du travail de l'agent ;
- Le télétravailleur ne doit pas influencer sur la configuration initiale du poste fournis par la SDSI, en particulier sur les paramètres techniques contribuant à leur sécurité. Cela concerne plus précisément la configuration des interfaces de communication réseau (modem 3G/4G, Wi-Fi, NFC, VPN, etc.), les paramètres de comptes (APN, messagerie, etc.) et la configuration des applications. En aucun cas, le télétravailleur ne doit désactiver ou débrayer le client VPN de chiffrement permettant de raccorder le terminal au système d'information de l'établissement lorsqu'il est mis en œuvre ;


		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

- Il doit prendre toutes les mesures nécessaires afin de prévenir le vol de l'ordinateur portable, l'usage du câble antivol fourni par l'établissement doit être systématique ;
- Il doit verrouiller sa session dès que l'équipement n'est plus utilisé ;
- Il faut éviter les comportements à risque tel que laisser l'ordinateur portable sans surveillance dans un lieu public ou un véhicule ;
- Il ne doit pas conserver de mot de passe inscrit sur des documents papiers dans la sacoche ou à proximité du poste de travail ;
- le filtre de confidentialité doit toujours être positionné sur l'écran afin de garantir la confidentialité des données traitées en dehors des locaux de l'établissement ;
- En cas de détérioration, de perte ou de vol, l'utilisateur doit alerter sans délai la SDSI via l'assistance informatique.

Article 8 : Travail en mode nomade

Toutes les recommandations liées au télétravail s'appliquent au travail en mode nomade. Certaines recommandations particulières doivent être suivies :

- Les réseaux Wi-Fi des cybercafés, des hôtels, des lieux publics et bureaux de passage n'offrent aucune garantie de sécurité et confidentialité, il est donc fortement déconseillé de s'y connecter à moins de disposer d'une solution de chiffrement VPN. Il est d'ailleurs préférable, si c'est possible, d'utiliser la fonction de partage de connexion de son smartphone professionnel;
- Il est en particulier formellement interdit de connecter un périphérique de l'établissement (PC portable, smartphone, tablette, etc.) au Wi-Fi public déployé dans les espaces de l'établissement ;
- Dans le cadre de voyages à l'étranger, il convient d'être encore plus vigilant du fait de la surveillance, quel que soit le régime politique, des centres d'affaires, hôtels et des réseaux. Dans certains pays, les chambres d'hôtel peuvent être fouillées sans que vous vous en rendiez compte. L'utilisateur doit se conforter au passeport de conseils aux voyageurs rédigé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

Article 9 : Confidentialité

Les agents de l'établissement doivent faire preuve d'une discrétion absolue dans l'exercice de leurs missions et se conformer au règlement intérieur en vigueur dans l'établissement.

Au titre des systèmes d'information de l'établissement :

L'accès aux informations et documents traités et conservés sur les systèmes d'information doit être limité aux stricts besoins. Il est interdit de prendre connaissance d'informations détenues par les droits d'autres utilisateurs, même si celles-ci n'ont pas été correctement protégées.

Il est interdit d'accéder à d'autres données internes de l'établissement que celles nécessaires à l'accomplissement de sa mission.

Le respect des règles d'éthique professionnelle, de déontologie, de l'obligation de réserve, du devoir de discrétion et de l'obligation de confidentialité implique de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations et données ;
- ne pas extraire ces informations et données confidentielles et ne pas les détourner de leur utilisation normale ;


La diffusion de contenus sur internet, en particulier au sein des réseaux sociaux et sur les blogs, peut engendrer des risques pour l'établissement. Il est donc strictement interdit de diffuser sur internet ou via des applications la moindre information à caractère professionnel.

Article 10 : Propriété Intellectuelle

L'utilisation des logiciels et plus généralement de tout document (fichier, image, son, vidéo) doit se faire dans le respect des droits de propriété intellectuelle et du droit à l'image et à la vie privée, des recommandations fixées par les détenteurs de droits et des engagements pris par l'établissement (dans les contrats de licences ou droit d'utilisation, par exemple).

En particulier, sans que cette liste soit exhaustive :

1. La reproduction de logiciel est interdite. Seul l'établissement d'une copie de sauvegarde pourra être autorisé par la SDSI.
2. Il est strictement interdit d'installer sur un équipement de l'établissement un logiciel ou une application, sans avoir obtenu l'accord préalable de la SDSI.
3. Le téléchargement, le visionnage en streaming ou le stockage d'œuvres protégées, sans autorisation des ayants droit, sont de nature à engager la responsabilité de l'établissement et sont donc strictement

			MDL
	Charte d'Utilisation des Moyens Informatiques		MDL - SSI
			1 - 0
			26/11/2020

interdits. L'établissement effacera des Systèmes d'Information toute trace de ces œuvres, introduites en violation des droits de propriété intellectuelle de tiers.

4. Il est strictement interdit de reproduire, copier, utiliser remettre à des tiers ou diffuser, les bases de données, pages web, dessins & modèles, logos ou autres créations de l'établissement ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits.
5. Il est strictement interdit de reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles.
6. Il est strictement interdit de reproduire, copier, utiliser ou diffuser des éléments susceptibles de porter atteinte à l'image ou à la vie privée des utilisateurs ou de toute autre personne

Article 11 : Obligations relatives aux données à caractère personnel


Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de Données Personnelles, 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 depuis le 25 mai 2018.

Dans ce cadre, les utilisateurs devront se conformer à la procédure en vigueur pour la mise en œuvre d'un traitement de Données Personnelles.

Conformément à la réglementation applicable en matière de 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 concernées ;
- le droit d'accès, de rectification ;
- le droit d'opposition ;
- le droit d'effacement ;
- la protection adaptée aux risques présentés par le traitement sur les plans technique et organisationnel ;
- le contrôle rigoureux de la diffusion de données à caractère personnel à l'attention de tiers extérieurs.

Toute création ou modification d'un traitement de Données Personnelles doit, préalablement à sa mise en œuvre, être déclarée auprès du DPD qui étudie en lien avec la cellule RGPD la pertinence des données recueillies, la finalité du traitement, les durées de conservation, les destinataires des données, le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour protéger les données. Le Délégué à la Protection des Données procède ensuite à l'inscription du traitement au registre des activités de traitement de l'établissement.

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

En cas de non-respect des obligations relatives à la réglementation sur la protection des données, l'établissement peut prendre toute mesure pour mettre fin au traitement de données illégal et sanctionner l'utilisateur.

Article 12 : Protection de l'image de l'établissement

Les faits et informations de l'établissement dans son fonctionnement n'ont pas à être rendus publics. Aucun fichier, quelle que soit sa nature, ne doit être diffusé vers l'extérieur et notamment sur internet, sans motif professionnel autorisé.

L'utilisateur doit faire preuve de mesure et de discrétion lorsqu'il s'exprime par l'intermédiaire des outils de communication. Il doit également s'abstenir de publier des messages contraires à l'ordre public, diffamatoires, racistes, xénophobes, homophobes, sexistes, injurieux, portant atteinte à la décence ou constituant une diffusion de fausses informations.


L'utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs lors de ses échanges électroniques par courrier ou par publication sur des forums professionnels. Il n'émettra pas d'opinions étrangères à son activité professionnelle susceptibles de porter préjudice à l'établissement.

Article 13 : Droit à la déconnexion

En application de la réglementation relative au droit à la déconnexion, l'établissement s'est doté d'une charte des temps qui symbolise son engagement pour l'équilibre des temps et la qualité de vie au travail.

Les utilisateurs doivent se déconnecter des moyens informatiques et outils numériques (comme par exemple les portables, tablettes, messageries, applications...) hors du temps de travail.

Concernant plus particulièrement l'usage de la messagerie électronique professionnelle, il est précisé que l'utilisateur n'est jamais tenu de prendre connaissance des courriers électroniques qui lui sont adressés ou d'y répondre en dehors de son temps de travail. Il en est de même des appels ou messages téléphoniques professionnels reçus pendant les temps de repos ou de congé, sauf cas d'urgence exceptionnelle ou d'astreinte professionnelle.

	Charte d'Utilisation des Moyens Informatiques	MDL
		MDL - SSI
		1 - 0
		26/11/2020

Article 14 : Conditions d'un usage privé

Bien que les moyens informatiques et outils numériques de l'établissement soient réservés à un usage professionnel, leur utilisation à des fins non professionnelles est admise pour répondre en cas d'urgence à des obligations socialement admises et/ou pour des usages exceptionnels et raisonnables.

Cette utilisation pourra faire l'objet de limitation voire de suspension en cas d'abus après information préalable de l'utilisateur.

Ainsi, une utilisation à titre privée est admise durant les temps de pause si :

- Elle ne perturbe pas la bonne exécution du travail de l'utilisateur, de ses missions professionnelles et la continuité du service ;
- Elle n'impacte pas les performances des systèmes ou leur sécurité ;
- Elle ne porte pas atteinte aux obligations qui incombent aux utilisateurs compte tenu de leur statut et notamment, les obligations de dignité, de loyauté, de discrétion, de neutralité ou de confidentialité ;
- Elle ne poursuit pas un but lucratif ou même ludique ;
- Elle est conforme à la réglementation en vigueur et à la présente Charte ;
- L'utilisateur n'utilise pas les moyens informatiques pour diffuser des informations à caractère illégal ;
- L'utilisateur n'implique pas l'établissement dans cet usage personnel des ressources et ne porte pas atteinte à son image de marque ou à sa réputation ;


L'usage non professionnel des moyens informatiques et outils numériques se traduit dans les faits par la possibilité d'enregistrer, de façon exceptionnelle et raisonnable, des fichiers privés sur le terminal mis à disposition de l'utilisateur par l'établissement ou d'utiliser un moyen de communication électronique de l'établissement.

Afin de garantir la confidentialité des répertoires et messages électroniques non professionnels, il est impératif que l'utilisateur utilise le terme « PRIVE » « Privé » « privé » « Prive » « prive » :

- sur le dossier informatique dans lequel il est contenu ;
- dans la zone objet du message électronique et le tiers destinataire du message devra être informé de cet usage ;
- si le moyen de communication utilisé ne comporte pas de champ « objet » (chat, messagerie instantanée, SMS, etc.), le message à caractère non professionnel doit débuter par le terme « PRIVE » « Privé » « privé » « Prive » « prive ».

A défaut d'utiliser le terme « PRIVE » « Privé » « privé » « Prive » « prive », tous les répertoires informatiques et tous les messages informatiques sont considérés comme professionnels.

L'utilisateur est entièrement responsable de son usage des moyens informatiques et outils numériques de l'établissement à des fins privées et le dégage en conséquence de toute responsabilité.


			MDL
	Charte d'Utilisation des Moyens Informatiques		MDL - SSI
			1 - 0
			26/11/2020

Par principe, le caractère non professionnel de l'usage des moyens informatiques et outils numériques interdit à l'établissement d'accéder aux contenus ou données émis, reçus ou échangés dans ce cadre.

Mais il ne fait pas obstacle à ce que :

- l'établissement puisse accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré pour ce dernier en termes notamment de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée ;
- ces éléments fassent l'objet de conservation technique dans le cadre de la mise en œuvre des sauvegardes, soit dans le cadre de back up ou de plans de continuité ou reprise d'activité mises en œuvre au sein de l'établissement ;
- en cas de détection ou de suspicion de la présence d'un code malveillant à la mise en quarantaine ou le cas échéant, à la suppression de l'élément quelconque qui comporte ou comporterait un code malveillant ;
- un administrateur, ou toute personne habilitée, accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des moyens informatiques et outils numériques, et ce, notamment, dans le cadre d'opérations de maintenance ;
- l'établissement peut, dans tous les autres cas, et pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors qu'il y est autorisé par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie, douanes, Commission nationale de l'informatique et des libertés (Cnil), notamment).

En tout état de cause, il est interdit de se connecter sur des sites à caractère pornographique, pédopornographique, zoophile, injurieux, violent, raciste, antisémite ou nazi, d'incitation à la haine ou à la violence ou à la commission d'acte illicite, discriminatoire, diffamatoire, faisant l'apologie du terrorisme, contrefaisant, ou manifestement contraire à l'ordre public ou de télécharger ou visionner ou stocker ou transmettre ou reproduire des contenus de telle nature.

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

Article 15 : Disposition en cas d'absence, de départ ou de décès d'un agent

Chaque utilisateur doit veiller à ce que la continuité du service soit assurée, conformément aux modalités d'organisation définies par l'établissement.

En cas d'absence ou de départ définitif de l'utilisateur et sur accord de l'utilisateur et autorisation de la Direction des Ressources Humaines, l'établissement se réserve le droit de mettre en place un système de délégation en l'absence d'accès permanent y compris pour les messages électroniques ou toute autre solution technologique permettant d'assurer la continuité de l'activité du service.

Absences :

En cas d'absence de l'utilisateur, pour quelle que raison et durée que ce soit, et sur autorisation de la Direction des Ressources Humaines, l'établissement se réserve le droit d'accéder directement aux différents dossiers, répertoires, courriels et, plus généralement, à tout document à caractère professionnel de l'utilisateur, ayant recours en tant que de besoin, aux codes administrateur systèmes.

En cas d'absence programmée de l'utilisateur, ce dernier s'engage à respecter la politique de message d'absence telle que prévue par l'établissement le cas échéant.


Départ :

A l'annonce du départ définitif d'un utilisateur de l'établissement, et pour des raisons légitimes de protection de ses intérêts, les droits d'accès et les conditions d'utilisation des moyens informatiques et des outils numériques pourront être modifiés. De même, des règles particulières de traçabilité pourront être mises en œuvre.

Au plus tard lors de son dernier jour de travail effectif dans les locaux de l'établissement, l'utilisateur doit :

- remettre en bon état général de fonctionnement, l'ensemble des moyens informatiques et outils numériques qui lui a été fourni ;
- restituer les moyens d'authentification ;
- supprimer la veille de son départ le répertoire et les messages électroniques nommés « PRIVE » « Privé » « privé » « Prive » « prive » ainsi que tous les documents de même nature. A défaut, et sauf procédure judiciaire ou enquête administrative, ces éléments sont automatiquement supprimés le lendemain du départ définitif de l'utilisateur de l'établissement, sans être consultés et sans qu'aucune copie ne soit réalisée ;
- à noter que le poste pourra être physiquement récupéré pour formatage.

A son départ définitif et sur autorisation de la Direction des Ressources Humaines, le compte de messagerie individuel de l'utilisateur peut suivre une procédure de reroutage vers le supérieur hiérarchique ou vers la personne qui le

	Charte d'Utilisation des Moyens Informatiques	MDL
		MDL - SSI
		1 - 0
		26/11/2020

remplace. Il est en outre mis en place un message d'absence. Le compte de messagerie est désactivé au bout d'un mois.

Décès :

En cas de décès de l'utilisateur, l'établissement conservera les données marquées « PRIVE » « Privé » « privé » « Prive » « prive » de l'utilisateur pendant une durée de six mois. La Direction des Ressources Humaines pourra les remettre aux ayants droit à première demande durant ce délai, sauf instruction écrite contraire de l'utilisateur.

Article 16 : Supervision des systèmes d'information

Les registres informatisés (conservés dans les systèmes d'information de l'établissement dans des conditions raisonnables de sécurité) sont considérés comme des preuves irréfragables de l'utilisation des moyens informatiques de l'établissement et des communications.

De ce fait, l'établissement met en œuvre des moyens permettant :


- le filtrage des sites Internet non autorisés (à caractère pédopornographique, xénophobe, etc.) ;
- le filtrage des sites Internet présentant un risque pour la sécurité, la performance, l'efficacité et la stabilité des systèmes d'information ;
- le déchiffrement des flux https dans le but légitime d'assurer la sécurité du système d'information en conformité avec les préconisations de la CNIL (non déchiffrement des sites banques, assurances, caisses de retraite, sécurité sociale, hôpitaux, cliniques, informations médicales,...) ;
- le blocage du téléchargement ou le visionnage d'œuvres protégées ;
- le contrôle a posteriori des données de connexion à internet ;
- le filtrage des mails venant de l'extérieur pour la sécurisation des échanges (antivirus et anti spam) ;
- l'élaboration de fichiers de journalisation des connexions afin de garantir une utilisation normale des ressources ;
- la prise en main à distance pour détecter et réparer les dysfonctionnements à distance du poste de travail.

D'autres entités, externes, à l'établissement sont également susceptibles de superviser et contrôler le trafic internet émanant de l'établissement tels que l'ANSSI, l'Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi), nos fournisseurs d'accès Internet.

L'établissement assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'il met à disposition, pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

Par conséquent, les applications de l'établissement, ainsi que les réseaux, messagerie et accès internet intègrent des dispositifs de traçabilité permettant d'enregistrer :

- L'identifiant de l'utilisateur ayant déclenché l'opération ;
- L'heure de la connexion ;
- Le système auquel il est accédé ;
- Le type d'opération réalisée ;
- Les informations ajoutées, modifiées ou supprimées des bases de données en réseau et/ ou des applications de l'établissement.

	Charte d'Utilisation des Moyens Informatiques	MDL
		MDL - SSI
		1 - 0
		26/11/2020

Le personnel de la SDSI est tenu au respect de la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises.

A des fins de maintenance informatique, la SDSI peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.

Dans le cadre de mises à jour et évolutions des systèmes d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, la SDSI peut être amenée à intervenir sur l'environnement technique des postes de travail.

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la réglementation applicable.

Article 17 : Respect de la Loi Informatique et liberté par l'établissement

L'établissement met en œuvre des traitements de Données Personnelles en relation avec l'usage des moyens informatiques et outils numériques couverts par la présente charte et pour assurer leur sécurité. L'établissement s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées.

L'établissement a désigné un Délégué à la Protection des Données.


Les catégories suivantes de données sont traitées :

- informations professionnelles ;
- informations relatives à l'identité ;
- image vidéosurveillance/vidéo protection ;
- log de connexion et autres traces ;
- informations sur l'utilisation des moyens informatiques et outils numériques.

Ces catégories de données proviennent essentiellement des moyens informatiques et outils numériques, ainsi que des annuaires informatiques et de la Direction des Ressources Humaines.

Ces données sont conservées pour les durées suivantes :

- les informations professionnelles, ainsi que les informations relatives à l'identité sont conservées le temps de présence de l'agent dans l'établissement augmentée des délais de prescription et de conservation obligatoire ;
- les informations sur l'utilisation des moyens informatiques et outils numériques ainsi que les logs de connexion et autres traces sont conservées selon les systèmes pendant une durée d' un an ;

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

- les images des systèmes de vidéosurveillance/vidéo protection sont conservées pendant une durée d'un mois sauf incident.

Ces données sont destinées à l'établissement, ainsi qu'aux personnes habilitées au sein de ce dernier et aux autorités compétentes.

Les traitements opérés dans le cadre de la charte ont pour finalité :


- le suivi et la maintenance des moyens informatiques et outils numériques, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;
- la gestion des annuaires et référentiels permettant de définir les autorisations d'accès aux applications et réseaux ;
- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des moyens informatiques et outils numériques, notamment la conservation des logs de connexion, des traces informatiques et des données de toutes natures notamment à des fins d'historisation et de preuve de l'utilisation des moyens informatiques et outils numériques ;
- la gestion de la messagerie électronique ;
- le fonctionnement en réseaux internes par métier ou par projet permettant la collecte, la diffusion ou la traçabilité de données de gestion des tâches, de la documentation, de la gestion administrative et des agendas des personnes répertoriées dans ces réseaux ;
- le contrôle du respect de la charte et les audits ;
- les statistiques ;
- les investigations et enquêtes.

Ces finalités permettent à l'établissement de poursuivre des intérêts légitimes liés à la bonne utilisation et à la sécurité de ses moyens informatiques et outils numériques dans le respect des droits des utilisateurs.

A toutes fins utiles, il est rappelé que les Données Personnelles collectées auprès des utilisateurs sont obligatoires aux fins de bonne gestion, d'organisation et de sécurité des moyens informatiques et outils numériques.

Conformément à la réglementation sur la protection des Données Personnelles, les utilisateurs sont informés qu'ils disposent d'un droit d'interrogation, d'accès, de rectification, d'effacement, de limitation, de portabilité et d'opposition au traitement des Données Personnelles les concernant et qui s'exerce auprès de la cellule RGPD (rgpd@louvre.fr).

Les personnes concernées peuvent également donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès. Une personne peut être désignée pour exécuter ces directives et elle aura alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre au responsable de traitement concerné. Lorsqu'il s'agit de directives particulières, elles peuvent également être confiées au responsable de traitement en cas de décès.

	Charte d'Utilisation des Moyens Informatiques	MDL
		MDL - SSI
		1 - 0
		26/11/2020

Les utilisateurs disposent d'un droit de réclamation auprès de la Cnil, autorité de contrôle en charge du respect des obligations en matière de protection des données à caractère personnel.

La réglementation sur la protection des données exige des responsables de traitement de données qu'ils notifient toute violation de données à caractère personnel à l'autorité compétente et, dans certains cas, qu'ils communiquent à la personne concernée par la violation. L'établissement a mis en place des procédures pour traiter toute violation présumée de Données Personnelles et notifie à la Cnil lorsqu'il est légalement tenu de le faire. Si un utilisateur soupçonne ou a connaissance d'une violation de données à caractère personnel, il ne doit pas tenter d'enquêter lui-même. Il doit immédiatement contacter la cellule RGPD (rgpd@louvre.fr) et suivre ses instructions. Il doit conserver toutes les preuves relatives à la violation potentielle de données à caractère personnel.

Article 18 : Responsabilité et sanction

L'utilisateur est responsable :

- dans le cadre de son activité professionnelle, de l'utilisation des moyens informatiques et outils numériques en conformité avec la présente Charte ;
- dans la sphère résiduelle de vie privée, de tout usage à caractère non professionnel à l'exclusion donc de toute responsabilité de l'établissement.

En cas de manquement grave de l'utilisateur à l'une des dispositions de la présente Charte, la SDSI rend compte immédiatement à la Direction des Ressources Humaines en communiquant les éléments de preuve nécessaires.


Toute mauvaise utilisation ou utilisation non conforme aux conditions et limites définies par la présente Charte est constitutive d'une faute.

En conséquence, le non-respect des dispositions légales et réglementaires, ainsi que de la présente Charte, expose l'utilisateur à des sanctions disciplinaires et/ou à des poursuites judiciaires.

En outre, l'utilisateur s'expose à des sanctions concernant son droit d'utiliser les moyens informatiques et les outils numériques notamment le contrôle renforcé, la suspension, le blocage, le retrait ou la suppression de son droit d'utiliser tout ou partie des moyens informatiques et outils numériques.

L'établissement, pour sa part, déclare mettre en œuvre, par le biais notamment de la présente Charte, tous les efforts nécessaires à un bon usage des moyens informatiques et des outils numériques et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des utilisateurs auxquels il fournit un droit d'accès.

La SDSI en concertation avec la Direction des Ressources Humaines se réserve le droit de procéder à la désactivation d'identifiants en cas de raisons légitimes après information préalable de l'utilisateur.

		MDL
	Charte d'Utilisation des Moyens Informatiques	MDL - SSI
		1 - 0
		26/11/2020

Article 19 : Entrée en vigueur

La présente charte est annexée au règlement intérieur de l'établissement et publiée sur l'intranet de l'établissement. Elle a été soumise pour avis au Comité d'hygiène, de sécurité et des conditions de travail le 04/11/2020 et au Comité technique le 06/11/2020, elle entrera en vigueur au 1^{er} janvier 2021.