UBO
Université de Bretagne Occidentale

CHARTE D'USAGE DES RESSOURCES INFORMATIQUES ET NUMÉRIQUES À L'UNIVERSITÉ DE BREST

sea·EU

La présente charte a été mise à jour le 12/01/2026 et approuvée lors du CA du 12/03/2026.

Sommaire

1 Préambule

L'Université de Brest (Université de Bretagne Occidentale (UBO)) met à disposition de ses utilisateurs et utilisatrices des ressources informatiques et numériques. Cette charte a pour but de définir les droits et devoirs de ces personnes vis-à-vis de ces ressources.

Points clés de la charte :

- **Accès aux ressources** : l'accès aux ressources est réservé aux étudiants et étudiantes, personnels et autres personnes autorisées, dans le cadre de leurs activités professionnelles ou académiques.
- **Utilisation des ressources** : l'utilisation des ressources doit être loyale, responsable et conforme aux lois et réglementations.
- **Sécurité des données** : vous êtes responsables de la sécurité des données que vous manipulez et devez respecter les règles de sécurité en vigueur. Vous êtes des acteurs clé de la sécurité.
- **Données personnelles** (RGPD) : l'UBO s'engage à respecter la réglementation relative aux données personnelles et à ne les utiliser que dans le cadre de ses missions. Vous vous engagez également à respecter cette réglementation.
- **Respect des règles** : le non-respect des règles de la charte peut entraîner des sanctions, telles que la suspension de l'accès aux ressources ou des sanctions disciplinaires.

Veuillez prendre connaissance de la suite de ce document pour une description détaillée de ces points.

2 Définitions

Les termes suivants sont utilisés dans le présent document et sont définis de manière à lever toute ambiguïté :

DPO ou Délégué à la Protection des Données : personne ou ensemble des personnes responsables de la conformité au Règlement Général sur la Protection des Données personnelles (RGPD), garant du respect des droits des personnes et conseiller de l'organisation sur la protection des données.

DSIUN : Direction des Systèmes d'Information et des Usages du Numérique, service central en charge de l'informatique et du numérique de l'UBO.

Référent informatique : informaticien ou informaticienne de proximité ou autre personnel dont la mission ou l'une des missions est d'assurer l'assistance informatique d'un ou plusieurs Usagers.

Ressources ou Ressources informatiques ou Ressources numériques ou Système d'information : tout ou partie des moyens matériels, logiciels, données, applications et systèmes de télécommunication mis en place par ou pour l'Université ou accessibles depuis son réseau. Ceci comprend notamment les postes de travail ou de consultation, logiciels, services en ligne, espace numérique de travail (ENT), outils numériques et de communication, réseaux.

RSSI ou Responsable(s) de la Sécurité des Systèmes d'Information : personne ou ensemble des personnes responsables de la définition de la politique de sécurité informatique au sein de l'établissement, de la définition des procédures associées et du contrôle de leur application.

Université ou UBO ou l'établissement : désigne l'Université de Brest.

Usager : désigne toute personne, quel que soit son statut, appelée à utiliser les Ressources informatiques. L'Usager peut être un personnel de l'UBO qu'il soit titulaire ou non, un étudiant ou une étudiante, un doctorant ou une doctorante, un post-doctorant ou une post-doctorante, une personne invitée ou hébergée, un intervenant ou une intervenante extérieur ponctuel ou régulier, un prestataire extérieur.

3 Objet de la Charte numérique

Dans le cadre de la mission de service public qu'elle remplit, l'UBO assure et facilite l'accès des Usagers aux Ressources du système d'information ainsi qu'aux ressources auxquelles il est possible d'accéder à distance, directement ou en cascade, à partir des réseaux de l'Université ou des moyens mis à disposition par elle ou pour elle.

A ce titre, elle se doit de :

- **respecter et faire respecter les lois et règlements** applicables, ses engagements contractuels et les règles déontologiques ;
- **assurer la sécurité de ces Ressources** : leur disponibilité, confidentialité, intégrité et éventuellement traçabilité.

La présente charte d'usage des Ressources informatiques et numériques à l'UBO, dite « charte numérique », définit les règles et les conditions d'utilisation des Ressources informatiques et numériques. Elle précise les droits et devoirs de l'Usager vis-à-vis de l'utilisation de ces Ressources et leurs conditions d'accès, dans le respect des lois et d'autrui.

Son non-respect engage la responsabilité personnelle de l'Usager.

4 Accéder aux Ressources numériques de l'UBO

→ **Qui peut utiliser les outils numériques de l'UBO ?**

→ **Comment obtenir un compte informatique ?**

→ **Quelles sont les règles d'utilisation des Ressources numériques ?**

L'accès et l'utilisation des Ressources numériques ne sont autorisés que dans le cadre des activités liées à la pédagogie, à la recherche, à l'orientation et à l'insertion professionnelle pour les étudiants et étudiantes, et des activités liées à l'activité de l'Université pour les personnes autorisées, tant internes qu' externes.

Cette utilisation et la connexion d'un équipement sur le réseau sont soumises à autorisation, notamment via la mise à disposition d'un compte informatique UBO. Cette autorisation est strictement personnelle et incessible. Elle peut être réduite ou suspendue à tout moment en cas de non-respect de cette charte. Cette autorisation prend fin lors de la cessation de l'activité qui l'a justifiée.

Les droits d'accès d'un Usager aux Ressources dépendent du statut et des missions de celui-ci et évoluent de concert avec ce statut et ces missions.

Un étudiant ou étudiante peut activer son compte informatique à partir de l'ENT, dès qu'il ou elle est inscrit dans l'établissement (inscription administrative).

Un personnel titulaire ou contractuel peut accéder aux Ressources numériques dès qu'il est connu de l'établissement (essentiellement au travers du système d'information des ressources humaines) et à partir du moment où un compte informatique lui est accordé.

Les autres personnels (hébergés, invités) doivent demander la création d'un compte informatique via le ou la responsable de l'unité d'accueil ou son RAF.

Tout Usager cesse de bénéficier de ce droit d'accès lorsque ses liens avec l'établissement se terminent et après une période de sursit. Il en est systématiquement informé par mail au préalable.

5 Utiliser les Ressources numériques de l'UBO en toute sécurité

→ **Protégez vos mots de passe**

→ **Se protéger des virus et des logiciels malveillants**

→ **Respectez la confidentialité des données**

Tout Usager est responsable de l'usage qu'il fait des Ressources numériques et contribue à son niveau à la sécurité des systèmes d'information. Il est un acteur clé de leur sécurité et de l'usage qui en est fait. A ce titre, il fait preuve de vigilance vis-à-vis des informations reçues, traitées ou transmises.

Il s'engage à utiliser les Ressources d'une manière licite, loyale et conforme à l'usage prévu, ceci afin d'en préserver l'accessibilité, la disponibilité, l'intégrité et la confidentialité. Il s'engage à ne pas apporter volontairement de perturbations au bon fonctionnement des Ressources numériques.

L'Usager s'engage à :

- **respecter les termes de cette charte informatique** ;
- **n'accéder qu'aux Ressources** pour lesquelles il a été dûment habilité et à ne transférer aucune donnée sur des moyens informatiques autres que ceux approuvés par l'Université ;
- **ne pas se livrer à des actions mettant sciemment en péril la sécurité** ou le bon fonctionnement des Ressources auxquelles il accède ;
- **ne pas mettre à la disposition d'utilisateurs non autorisés** un accès aux Ressources de l'Université ;
- **ne communiquer d'informations ou de droits d'accès** à ces informations qu'aux personnes ayant besoin d'en avoir connaissance ;
- **ne pas usurper l'identité d'un tiers** ni masquer sa véritable identité ;
- **ne pas se connecter ou essayer de se connecter à une Ressource** autrement que par les dispositifs prévus ou sans y être autorisé par le ou la responsable de celle-ci ;
- **ne pas contourner ou essayer de contourner les systèmes de protection** mis en place sur les Ressources ;
- **se renseigner auprès de son Référent informatique** sur les règles en vigueur pour toute installation de logiciel et n'installer ou faire installer que les logiciels prévus dans le cadre de ses rôles ou missions ;
- **choisir des moyens d'authentification personnel**s (mots de passe) sûrs et respectant les bonnes pratiques en vigueur, les garder secrets et ne les communiquer en aucun cas à des tiers ;
- **signaler à son responsable ou son Référent informatique, toute tentative de violation de son compte** et, de façon générale, toute anomalie qu'il peut constater ;
- **ne pas quitter son poste de travail ni ceux en libre-service en laissant des Ressources ou services accessibles** (il doit alors fermer sa session ou la verrouiller si son absence est temporaire) ;
- **s'imposer le respect des lois** et notamment celles relatives aux publications à caractère illicite, injurieux, raciste, pornographique, diffamatoire, ainsi que le respect des principes de neutralité religieuse, politique et commerciale ;
- **respecter les principes de confidentialité** des correspondances et de propriété intellectuelle ;
- **ne pas installer ou utiliser des logiciels non officiels ou modifiés** (logiciels pirates).

> **L'informatique en nuage** (« cloud computing ») fournit de nouvelles opportunités en matière d'étalement numérique mais emporte de nouveaux risques pour le Système d'information.

L'Usager veillera donc à :

- **ne pas transférer ou stocker les données de l'Université** sur des Ressources autres que celles validées par l'Université[1] ;
- **ne partager des données** (notamment celles issues des espaces partagés) qu'avec des destinataires dûment identifiés, limiter l'accès aux seules données nécessaires et révoquer le partage dès que possible ;
- **ne pas procéder à des traitements de masse** entre des équipements dans ou hors du réseau UBO, sans l'avis express de la DSIUN.

Les réseaux wifi sont un moyen aisé d'accéder au réseau internet et à celui de l'Université. Des réseaux wifi trompeurs (WiFi phishing ou Evil Twin) dont l'objectif est d'accéder aux ressources de l'Usager peuvent cependant exister.

L'Usager veillera donc à n'utiliser que les réseaux wifi « eduroam » ou « invité » s'il est dans l'enceinte d'une université française ou un réseau wifi connu et sûr s'il est à l'extérieur (wifi de box internet pour le télétravail, par exemple). Dans tous les autres cas, il évitera d'utiliser son mot-de-passe et d'accéder ou transférer des données confidentielles ou sensibles qui pourraient être révélées.

6 Accéder aux Ressources de l'UBO depuis l'extérieur

→ **Respectez les mêmes règles que sur le réseau interne**

→ **Dissociez les usages personnels et professionnels**

→ **N'utilisez que des logiciels approuvés**

L'accès depuis un réseau externe à l'Université vers les Ressources de celle-ci, doit respecter les mêmes règles de base que depuis le réseau interne.

Les Usagers en télétravail doivent séparer usage privé et usage professionnel : matériels distincts, mots de passe différents.

L'accès depuis l'extérieur aux Ressources de l'Université étant particulièrement critique en matière de sécurité, l'Usager doit tout particulièrement veiller à :

- **Utiliser un mot-de-passe robuste** et ne pas le communiquer à un tiers ;
- Depuis un matériel en libre-service (cyber café, bibliothèque, etc.), **se déconnecter de l'ENT** et de tout autre service en fin d'accès, **ne pas enregistrer son identifiant sur le navigateur**, fermer les applications ouvertes et sa session de travail ;
- **Utiliser une connexion sécurisée** (par exemple, HTTPS pour le web) pour accéder aux services en mode web ;
- **Utiliser le réseau privé virtuel** (VPN) fourni par l'UBO entre un matériel UBO et le réseau interne UBO, et seulement dans ce cas ;
- **Utiliser les équipements fournis par l'Université** pour toute activité professionnelle, sur site comme en situation de télétravail ;
- **N'installer que les logiciels fournis par l'Université**, sauf autorisation explicite contraire ;
- **N'installer que les logiciels fournis par l'Université** que sur les seuls équipements fournis par elle, sauf autorisation explicite contraire.

1 Selon la criticité des données, l'usage pourra être interdit ou nécessiter un chiffrement obligatoire. Se rapprocher du Responsable Sécurité des Systèmes d'Information (RSSI) de l'UBO pour définir les mesures à adopter.

7 Messagerie et communication

→ **Utilisez votre adresse email professionnelle**

→ **Envoyer et recevoir des emails**

→ **Communiquez de manière responsable**

L'UBO met à la disposition de l'Usager **une ou plusieurs boîtes aux lettres professionnelles** ou académiques lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation des adresses électroniques associées se fait sous la responsabilité de l'Usager.

L'aspect nominatif de l'adresse électronique individuelle constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel ou académique de la messagerie.

L'Usager utilise ses coordonnées professionnelles ou académiques, en particulier son adresse électronique ou autre identifiant, avec précaution. En les utilisant sur des sites sans rapport avec son activité, il facilite les atteintes à sa réputation, à la réputation de l'UBO et prend le risque que son courriel ne soit pas reçu (spam).

L'Usager privilégie la boîte aux lettres électronique professionnelle lors de l'émission de courriels professionnels ou académiques. Corrélativement, il privilégie l'utilisation d'une boite aux lettres personnelles (non UBO) pour ses échanges privés.

Il évite d'émettre des opinions personnelles étrangères à son activité professionnelle et susceptibles de porter préjudice à l'Université, et fait preuve de la plus grande correction à l'égard de ses interlocuteurs dans ses échanges électroniques de toute nature.

Tout message reçu doit, par définition, **être considéré avec précaution**, notamment lorsque l'émetteur est inconnu, lorsque le contenu du message est inhabituel ou introduit un sentiment fallacieux d'urgence.

8 Utilisation personnelle des Ressources

Les Ressources numériques fournies à l'Usager par l'UBO sont réservées à l'exercice de son activité professionnelle ou académique.

Un usage personnel de ces Ressources est toutefois toléré aux conditions qu'il :

- reste marginal ;
- n'affecte pas l'usage professionnel ou académique ;
- ne mette pas en danger le bon fonctionnement et la sécurité du Système d'information ;
- n'enfreigne pas la loi, les règlements et les dispositions internes.

Toute donnée du Système d'information est présumée professionnelle et demeure à la disposition de l'Université, à l'exception des données explicitement désignées par l'Utilisateur comme ayant un caractère privé.

Pour la messagerie, il convient de mentionner « privé » (ou « personnel » ou « perso ») dans le champ « objet » des messages électroniques et dans les dossiers où ces messages sont conservés.

De même le stockage de données à caractère privé doit se faire en mentionnant le caractère privé sur la Ressource utilisée (dans un répertoire nommé « privé », « personnel » ou « perso », par exemple).

Cet espace personnel ne doit pas contenir de données à caractère professionnel et il ne doit pas occuper une part substantielle des ressources. La protection et la sauvegarde régulière des données à caractère privé incombent à l'Usager.

L'Usager est responsable des données à caractère privé qu'il conserve et il lui appartient de les détruire au moment de son départ. En cas de circonstances exceptionnelles (départ impromptu ou décès), l'UBO ne conserve ces données que pour une période limitée, permettant à l'Usager ou ses ayants droits de récupérer les informations personnelles qui s'y trouvent.

L'Usager s'interdit d'installer tout logiciel à usage personnel sur le ou les équipements professionnels mis à sa disposition pour son activité au sein de l'UBO.

9 Matériel personnel

→ **Usage autorisé sous la responsabilité de l'Usager**

→ **Son usage professionnel est prohibé**

Les Ressources numériques personnelles (en anglais : BYOD ou Bring Your Own Device), lorsqu'elles sont utilisées pour accéder aux Systèmes d'Information de l'UBO, ne doivent pas remettre en cause ou affaiblir les politiques de sécurité en vigueur dans l'Université par une protection insuffisante ou une utilisation inappropriée.

L'Usager reste seul responsable de l'utilisation qui est faite de son matériel personnel et en assure seul la gestion, les mises à jour et la sécurité.

Il protège les équipements personnels qu'il utilise pour, notamment, accéder, à distance ou à partir du réseau local, aux Ressources de l'UBO et l'équipe d'une protection contre les logiciels malveillants (anti-virus) à ses propres frais.

Il n'introduit pas de supports de données (clé USB, disque, etc.) sans respecter les règles de l'UBO et prend les précautions nécessaires pour s'assurer de leur innocuité.

Le stockage de données professionnelles sur un équipement personnel est à proscrire.

10 Données personnelles et vie privée

→ **Quels sont vos droits concernant vos données personnelles ?**

→ **Quels sont vos devoirs concernant ces données ?**

→ **Comment l'UBO protège vos données personnelles ?**

Une donnée à caractère personnel (DCP) est constituée de toute information relative à une personne physique.

Toute manipulation – y compris la création, la destruction, le stockage, le transfert ou le croisement – de DCP est soumis aux formalités préalables prévues par la loi « Informatique et Libertés » et le Règlement Général sur la Protection des Données à caractère personnel (RGPD).

En conséquence, tout Usager souhaitant procéder à un tel traitement devra rechercher l'avis du Délégué à la Protection des Données (DPD, aussi appelé DPO pour Data Protection Officier) et se conformer aux règles du RGPD (loi du 25 mai 2018). Il en fera déclaration préalable adressée au DPD/DPO de l'UBO (dpo@univ-brest.fr).

Les droits des personnes concernées :

- **Toute personne dispose d'un droit à l'image** et peut donc s'opposer, sauf obligation réglementaire ou juridique, à l'utilisation de celle-ci sans son consentement explicite.
- **Il ne peut être procédé au traitement de données à caractère personnel** que sur une base légale déterminée et pour une ou des finalités explicitement définies.
- **Le droit à l'accès aux informations personnelles et le droit de rectification** : chaque personne dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant.
- **Le droit à l'oubli** : chaque personne dispose d'un droit de retrait de certaines informations.
- **Le droit d'opposition** : chaque personne dispose d'un droit de s'opposer à ce que certaines données le concernant soient diffusées, transmises ou conservées.
- **Ces droits peuvent être limités** dans certains cas (notamment sécurité publique, exigences légales, gestion contractuelle, préservation des droits et libertés d'autrui).

L'UBO conserve et traite certaines de vos données personnelles dans le cadre de sa mission de service public et de ses obligations légales. Elle s'engage à ne faire cela que dans ce cadre et à obtenir votre accord explicite pour tout autre usage.

Après votre départ de l'établissement, elle procède automatiquement à la suppression d'une partie d'entre elles (notamment le contenu de messagerie, vos fichiers personnels) mais en conserve certaines (relevés de diplômes, historique de paie, par exemple) conformément à ses obligations réglementaires.

11 Utilisation de l'IA générative

→ **Respectez la Charte de l'IA générative de l'UBO**

L'intelligence artificielle générative (IAg) permet de créer de nouveaux contenus, tels que des textes, des images, des vidéos et de la musique, et d'enrichir des données existantes. Si elle présente un potentiel certain pour la recherche et l'enseignement, elle présente également des risques et des limites dont l'Usager doit avoir conscience.

La « Charte de l'IA générative » de l'UBO, annexée à la présente charte, s'applique et l'Usager s'engage à en respecter tous les principes et règles.

En voici, pour mémoire, les principaux principes :

- **Respect des lois et réglementations** : l'utilisation de l'IA générative doit respecter les lois et réglementations en vigueur, notamment en matière de propriété intellectuelle, de protection des données personnelles et de lutte contre la désinformation.
- **Responsabilité et éthique** : l'Usager doit être conscient des implications éthiques de cette technologie et l'utiliser de manière responsable. Il doit notamment s'assurer que les contenus générés ne sont pas discriminatoires, haineux ou incitant à la violence.
- **Transparence** : l'Usager doit être transparent quant à l'utilisation de cette technologie. Il doit notamment indiquer clairement que les contenus générés sont le résultat total ou partiel d'un processus d'IA et non d'une création humaine.
- **Qualité et fiabilité** : l'Usager doit s'assurer que les contenus générés sont de qualité et fiables. Il doit notamment prendre les mesures nécessaires pour éviter la génération de contenus erronés ou trompeurs.
- **Confidentialité** : les données à caractère personnel ou confidentielles (données économiques ou liées à le recherche) ne doivent pas être soumises à une IAg non validée par l'établissement.
- **Décision automatique** : l'IAg – et plus généralement l'IA – ne peut être l'origine d'une décision automatique concernant une ou des personnes.

12 Sécurité des données

→ **Protégez vos données selon leur criticité**

→ **Limitez les droits d'accès donnés à une autre personne**

→ **Ne pas accéder à celles des autres sans autorisation**

→ **Que faire en cas de déplacement à l'étranger ?**

→ **Alertez en cas de doute**

L'Usager protège les données qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité.

Par données à caractère sensible, il faut entendre les données dont le maintien du secret présente un intérêt digne de protection, en particulier les informations relatives aux données à caractère personnel, à la garantie de la propriété intellectuelle (dépôt de brevet, secret industriel,...), à la protection du patrimoine scientifique et technique.

Dans le cadre de la manipulation de données à caractère sensible, il convient d'être vigilant lors de l'utilisation des outils et des réseaux informatiques. En particulier, ces données ne doivent pas circuler en clair sur le réseau, ne doivent être accessibles que par les personnes habilitées, et doivent être chiffrées si possible. Contactez le Responsable Sécurité des Systèmes d'Information (RSSI, rssi@univ-brest.fr) pour vous fournir une analyse et des conseils sur les outils adaptés.

Lorsqu'il crée une donnée ou un document, l'Usager détermine son niveau de sensibilité et applique les règles permettant de garantir sa protection durant tout son cycle de vie (marquage, stockage, utilisation, transmission, impression, suppression, etc.)

Par défaut et sauf mention contraire, toutes les données manipulées par l'Usager doivent être considérées par lui comme sensibles et protégées en conséquence.

Afin de se prémunir contre les risques de vol de documents sensibles, l'Usager s'assure que ses documents papier et ses matériels sont sous sa surveillance directe ou mis en sécurité et que, s'il y a lieu, son poste de travail est verrouillé.

Lorsqu'il stocke ou manipule des données à caractère sensible, l'Usager en mobilité – notamment lors de déplacements à l'étranger – veille tout particulièrement à leur sécurité :

- **en chiffrant par défaut le disque dur** de son ordinateur,
- **en limitant les données** qu'il emporte,
- **en utilisant un ordinateur vierge** de données sensibles.

Ces données ne doivent pas être transférées ou stockées sur des équipements personnels.

A l'étranger, l'Usager veille à n'accéder aux Ressources numériques de l'UBO qu'au travers d'une connexion sécurisée (via le mode HTTPS pour le web ou un réseau privé virtuel / VPN), depuis un équipement sûr, et à ne transférer que les données strictement nécessaires.

13 Devoirs de signalement et d'information

→ **Mettre en place les moyens de sécurité**

→ **Alerter en cas d'anomalie ou de doute**

Pour prévenir les vols, l'Usager s'engage à utiliser les moyens de protection disponibles (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour garantir la protection des équipements mobiles et des informations qu'ils renferment (ordinateur portable, clé USB, ordiphone, tablette, etc.)

De même, il maintient à jour les logiciels mis à sa disposition et installe ou fait installer les mises à jour de sécurité qui visent à corriger les failles de sécurité qui pourraient apparaître. Il s'engage à ne pas désactiver ou faire désactiver les mesures de sécurité logique (outils de détection et de réponse aux activités suspectes, anti-virus, par exemple) installées sur son matériel.

L'Usager qui a connaissance d'un dysfonctionnement ou d'une anomalie (telle qu'une intrusion dans le système d'information ou la suspicion d'une usurpation d'un code d'accès), doit en avertir sans délai son Référent informatique ou son responsable.

De même, l'Usager doit signaler le plus rapidement possible à son Référent informatique ou son responsable toute perte ou tout vol d'un équipement mis à sa disposition.

Les alertes de sécurité doivent être signalées au RSSI de l'établissement (rssi@univ-brest.fr).

14 Analyse et contrôle de l'utilisation des Ressources

→ **Enregistrement des traces de fonctionnement et de télémétrie**

→ **Durée de conservation**

L'usage du Système d'information et la réglementation imposent de mettre en œuvre une diversité de mesures de sécurité afin d'assurer une protection adéquate des Ressources, parmi lesquelles la sauvegarde régulière des données, le filtrage des accès et l'enregistrement automatique d'évènements (fichiers de journalisation de l'activité) à des fins de contrôle, de statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Ces moyens sont opérés dans le respect de la législation applicable et notamment du RGPD, exclusivement par les personnels habilités.

Ces données ne sont utilisées que pour la ou les finalités pour lesquelles elles ont été collectées et les personnels habilités pour réaliser ces tâches d'administration et de supervision sont soumis au secret professionnel.

Elles sont automatiquement supprimées passé un délai (1 an pour les sauvegardes, 6 mois à 1 an pour les fichiers de journalisation).

15 Mesures prises en cas de non respect de la charte

Le non-respect des règles définies dans cette Charte pourra donner lieu, indépendamment des éventuelles sanctions pénales telles que prévues par les lois et règlements en vigueur, à la mise en œuvre des mesures suivantes :

- **Limitation ou suspension de l'accès aux Ressources**, à titre conservatoire ;
- **Sanctions disciplinaires** telles que définies par le code de l'éducation.

En cas d'urgence, la DSIUN peut être amenée à :

- **Limiter ou interrompre temporairement l'accès d'un Usager** aux Ressources de l'Université ;
- **Isoler ou neutraliser provisoirement toute donnée**, serveur ou fichier manifestement non conforme aux dispositions de la présente Charte ou qui mettrait en péril la sécurité des Ressources numériques.

16 Révision

Les Usagers seront avisés de toute modification de la présente charte par une publication de celle-ci sur le site internet de l'UBO et par un message d'information diffusé sur les listes officielles de messagerie de l'UBO.

Université de Bretagne Occidentale

DSIUN
Direction des Systèmes d'information
et des Usages du numérique