CHARTE D'UTILISATION DES RESSOURCES ET MOYENS NUMERIQUES DE L'UNIVERSITE DE TECHNOLOGIE DE BELFORT-MONTBELIARD

1- CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication de l'UTBM.
La charte informatique de l'UTBM est accessible notamment en ligne sur l'espace numérique de travail (ENT) de l'UTBM.

2- REGLES D'UTILISATION DU SYSTEME D'INFORMATION DE l'UTBM

• Authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son arrivée à l'UTBM. Un mot de passe est associé à cet identifiant de connexion. Les moyens d'authentification sont personnels et confidentiels.

L'UTBM préconise une composition de mot de passe constitué de 8 caractères minimum combinant chiffres, lettres et caractères spéciaux. Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé régulièrement.

• Règles de sécurité

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

- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail ni installer de logiciels sans habilitation explicite délivrée par la Direction des Systèmes Informatiques (DSI).
- Ne pas copier, modifier, détruire les logiciels et les données propriétés de l'UTBM.
- Verrouiller son ordinateur dès qu'il quitte son poste de travail.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.

L'utilisateur a le devoir de signaler toute tentative d'intrusion dans le système d'information ou toute menace pesant sur lui, s'il en a connaissance.

• Equipements nomades

On entend par « équipements nomades » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou Smartphones, CD ROM, clé USB etc.).
Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.
L'utilisation de Smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Lorsque ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être impérativement verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

3- DONNEES CONTENUES SUR LES EQUIPEMENTS MIS A DISPOSITION DE L'UTILISATEUR

Conformément au respect du principe de la continuité du service public auquel est astreinte l'UTBM, dans des circonstances exceptionnelles et dans l'hypothèse ou les données ne figurent pas dans un espace partagé, le responsable du laboratoire, du département ou du service concerné pourra contacter la direction qui saisira la DSI afin d'accéder aux données professionnelles contenues sur les équipements de l'utilisateur, en cas d'impossibilité ou d'incapacité de celui-ci.
La DSI est tenue d'en informer le correspondant informatique et liberté (CIL) qui inscrira ces interventions dans son registre. Le CIL communiquera la nature des opérations effectuées à la personne concernée ainsi qu'à toute personne qui en fera la demande écrite.

Les données et / ou fichiers informatiques contenus sur les disques durs locaux des équipements ou sur les serveurs de l'UTBM sont présumés être de nature professionnelle.

L'utilisateur doit veiller à la confidentialité des données contenues sur les équipements informatiques mis à sa disposition au regard des directives et recommandations de sécurité en vigueur dans l'établissement (recommandations ministérielles, de l'UTBM dans une politique de sécurité des systèmes d'information UTBM) ou au regard des engagements contractuels pris par l'UTBM.

L'utilisateur est autorisé ponctuellement à stocker des données personnelles sur l'équipement mis à sa disposition.

L'UTBM ne pourra en aucun cas être tenu pour responsable de la perte ou la destruction des données personnelles de l'utilisateur.
L'UTBM ne pourra en aucun cas accéder aux données personnelles de l'utilisateur, sous réserve que les fichiers ou dossiers de fichiers concernés soient désignés explicitement par l'utilisateur par les termes « personnel » « privé » ou « confidentiel ».

4- USAGE DE L'INTERNET

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.
Toutefois, une consultation résiduelle pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, et à l'ordre public est admise. Cette consultation pour des motifs personnels ne doit pas nuire au bon fonctionnement du service.
Tout téléchargement de fichiers, notamment de sons ou d'images, doit s'effectuer dans le respect des droits de propriété intellectuelle.

5- MESSAGERIE ELECTRONIQUE DE L'UTBM

• Utilisation de la messagerie électronique

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel.
Le contenu de la messagerie est présumé être professionnel.
L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique de l'UTBM.

Si les libertés d'opinion et de conscience ne peuvent être en aucun cas limitées, certains de leurs modes d'expression le sont.
L'utilisateur est soumis à une obligation de réserve et de confidentialité à l'égard des documents auxquels il a accès. 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.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions législatives, dont celles portant sur la liberté d'expression des contenus portant atteinte à la vie privée (atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, l'injure publique, protection du droit d'auteur, des marques…).

L'ensemble des messages relevant de la communication institutionnelle (en interne ainsi qu'en externe) de l'UTBM sont soumises à la validation du service communication avant diffusion.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de l'UTBM : ces adresses ne peuvent être utilisées sans autorisation explicite. Les messages envoyés dans ce cadre pourront faire l'objet d'une modération.

Conformément au respect du principe de la continuité du service public auquel est astreinte l'UTBM, dans des circonstances exceptionnelles et dans l'hypothèse où les données ne figurent pas dans un espace partagé, le responsable du laboratoire, du département ou du service concerné pourra contacter la direction qui saisira la DSI afin d'accéder à la messagerie professionnelle de l'utilisateur, en cas d'impossibilité ou d'incapacité.
La DSI est tenu d'en informer le correspondant informatique et liberté (CIL) qui inscrira ces interventions dans son registre. Le CIL communiquera la nature des opérations effectuées à la personne concernée ainsi qu'à toute personne qui en fera la demande écrite.

Cependant, afin de respecter le droit au respect de la vie privée ainsi que le principe du secret des correspondances privées, aucun accès ne sera rendu possible par le CRI aux messages qui comporteront la mention expresse ou manifeste de leur caractère personnel ou les messages classés dans un dossier « personnel » ou « confidentiel » à la racine de l'arborescence de la messagerie.

• Courriel non sollicité

L'UTBM dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

6- TELEPHONES

L'UTBM met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.
L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.

Des restrictions d'utilisation par les agents des téléphones fixes sont mises en place en tenant compte de leurs missions. A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

L'UTBM s'interdit de mettre en œuvre un suivi détaillé de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants.

Toutefois, en cas d'utilisation manifestement anormale, le service concerné, sur demande du directeur de l'UTBM, se réserve le droit d'accéder aux numéros complets des relevés individuels.

7- ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information de l'UTBM, différents dispositifs sont mis en place.

• Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour l'UTBM et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, messagerie instantanée....).

• Les systèmes automatiques de traçabilité

La DSI opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité. Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'évènement. Le service informatique est le seul utilisateur de ces informations qui sont effacées à l'expiration d'un délai de trois mois.

• Gestion du poste de travail

A des fins de maintenance informatique, la DSI peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur. Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, la DSI peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

8- PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR

Lors de son départ, l'utilisateur doit restituer au département, laboratoire, service d'affectation l'ensemble des matériels mis à sa disposition.
Il doit préalablement effacer ses fichiers et données privées et restituer à son département, laboratoire, service d'affectation l'ensemble des dossiers numériques professionnels dont il a eu la charge.
Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum de six mois après son départ.

9- RESPECT DE LA PROPRIETE INTELLECTUELLE

L'utilisation des ressources informatiques implique le respect du droit de propriété intellectuelle.
En conséquence, chaque utilisateur doit :

- Utiliser les logiciels dans les conditions des licences souscrites ;
- Ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

10- RESPONSABILITES - SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

Par ailleurs, l'utilisateur est conscient que le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information est susceptible d'entraîner l'application de sanctions pénales.

11- PROTECTION DES DONNEES A CARACTERE PERSONNEL

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. L'UTBM a désigné un correspondant à la protection des données à caractère personnel. Il est obligatoirement consulté par le responsable des traitements préalablement à leur création.

12- ENTREE EN VIGUEUR DE LA CHARTE

La présente charte a été adoptée par le conseil d'administration de l'UTBM, en date du 25 septembre 2014 et annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'information de l'UTBM.
Conformément à l'article 52 du règlement intérieur de l'UTBM, cette charte complète le règlement intérieur.

Contacts :

Direction de l'UTBM : direction@utbm.fr
Centre de ressource informatique : http://Monespace.utbm.fr
Correspondant Informatique et Liberté : cil@utbm.fr
Responsable Sécurité des Systèmes Informations : rssi@utbm.fr