

## 6.2 La sauvegarde des données

La sauvegarde des données a deux principaux objectifs:

**L'intégrité:** garantir que les données ne soient pas corrompues par un agent extérieur

**La disponibilité:** permettre de maintenir la continuité de service. La sauvegarde permet une restauration plus rapide de votre système d'information.

## 6.3 Mise en place d'une politique de sauvegarde des données

La sauvegarde des données informatiques doit se faire régulièrement sur un support différent de celui où sont stockées habituellement les données.

La sauvegarde doit permettre la restitution des données « brutes », des comptes utilisateurs, des droits d'accès aux données et ressources.

La sauvegarde des données ne doit pas empêcher les utilisateurs d'utiliser le système d'information.

La plupart des applications ont un utilitaire de sauvegarde

## 7 Respectez la loi

La loi est applicable sur internet, comme dans la vie courante : un délit sur internet est passible de la même peine qu'un délit « réel ». Le code civil est complété par des textes spécifiques (Loi Economie Numérique pour les FAI et hébergeurs) et textes réglementaires pour l'éducation notamment.

Attention : la plupart du temps les établissements scolaires sont aussi considérés comme hébergeurs et fournisseurs d'accès.

<http://www.cnil.fr/>

<http://www2.educnet.education.fr/legamedia>

## 8 Protégez les mineurs

8.1 Obligation d'utiliser un pare-feu Amon avec système de filtrage et système d'authentification pour les accès internet.

8.2 Mise en place de chartes de bon usage des réseaux et d'internet

8.3 Affichette à placer dans chaque lieu où les mineurs peuvent avoir un accès à internet : <http://sicep.ac-dijon.fr/spip.php?article55>

8.4 Chaîne d'alerte:

Elle repose sur les **chefs d'établissement** (Les modalités de mise en œuvre du dispositif de filtrage sont sous sa responsabilité et sur une **cellule académique** (Elle centralise les remontées d'informations concernant les sites inappropriés accessibles).

8.5 Dès qu'un site inapproprié est repéré :

**Avertir le chef d'établissement**

**Inscrire le lien du site repéré** aux adresses suivantes : <http://aiedu.education.fr/>, et [securite.internet@ac-dijon.fr](mailto:securite.internet@ac-dijon.fr)

**Bloquer l'accès du site sur le pare-feu AMON :** <http://sicep.ac-dijon.fr/spip.php?article67>

## 9 Cherchez des informations

Intranet académique: <http://www.dijon.men.fr> :

Serveur SICEP : <http://sicep.ac-dijon.fr>

**Si vous ne trouvez pas !**

Serveur d'assistance: <https://extranet.ac-dijon.fr/assistance/>

## 10 Demandez du secours

**10.1 Le QOQQC :** Quoi ? Où ? Qui ? Quand ? Comment ? ; Simple et rapide d'utilisation, le QOQQC est un questionnaire méthodique permettant d'analyser une situation et de donner les bons renseignements au service d'assistance.

**Quoi :** PC, serveur, routeur

**Où :** local technique CDI, secrétariat

**Qui :** professeur, gestionnaire...

**Quand :** maintenant, hier, répétitif...

**Comment :** après une opération, après allumage...

### 10.2 Avant de faire une demande d'assistance

Se renseigner en interne,

Trouver les informations techniques et de sécurité sur l'**Intranet académique:** <http://www.dijon.men.fr> et <http://sicep.ac-dijon.fr>

### 10.3 Qui fait la demande d'assistance ?

La demande doit être faite par le gestionnaire du réseau administratif ou le correspondant TICE.

**10.4 Pour tous problèmes techniques ou conseils : Serveur d'assistance:** <https://extranet.ac-dijon.fr/assistance/> :

**10.5 Pour tous problèmes d'accès à l'intranet** (connexion impossible) et accès à la messagerie (login et mot de passe) :

**Ligne d'assistance:** 03 80 44 88 09

**10.6 En cas de panne « internet » :** télécopie : 03 80 44 88 91

### 10.7 Que faire si vous êtes contaminé par un virus?

Débrancher le câble du réseau (la machine ne contaminera pas d'autres PC, prévenir le Service d'assistance.

C.E.T.I.A.D

Messagerie : [cetiad@ac-dijon.fr](mailto:cetiad@ac-dijon.fr)

Conception/Réalisation

Francis Bordes CETIAD/SICEP

# TIC SUR DIX

10 repères importants pour  
l'utilisation des T.I.C. en E.P.L.E.



## 1 Connectez-vous ! Un login, un mot de passe-

Il est strictement personnel : ne le confiez à personne.

### Quels comptes, pour quoi !

Compte de messagerie personnelle :

Messagerie académique, I-Prof, SCONET,  
Serveur d'assistance

Compte de messagerie de l'établissement

Messagerie de l'établissement

Comptes utilisateurs du réseau administratif

Accès au réseau

Administration d'Horus et Amon

Comptes utilisateurs du réseau pédagogique

Accès au réseau

Compte d'accès aux applications

ETIC, @SSR, GIBII

### Les paramètres de comptes à conserver au coffre !

Comptes d'administration du réseau administratif

Administration d'Horus et Amon

Comptes d'administration du réseau pédagogique

Administration du serveur pédagogique et  
serveur DMZ, administration des applications  
installées sur ces serveurs.

## 2 Utilisez correctement le réseau :

**2.1 Regrouper les éléments Switchs, Routeur, Pare-feu, serveurs** dans un local technique unique. Protéger physiquement les locaux techniques. Protégez électriquement les éléments actifs et les serveurs par des onduleurs. Ces locaux doivent être aérés, la température ne devant pas excéder 35 °C.

**2.2 S'authentifier et s'identifier** de manière fiable : mot de passe de qualité : ([www.dijon.men.fr/intranet/InfosAca/Securite/Page/Securite.htm](http://www.dijon.men.fr/intranet/InfosAca/Securite/Page/Securite.htm))

**2.3 Avoir un anti-virus à jour sur les postes**

**2.4 Mettre à jour les systèmes.**

**2.5 Se déconnecter systématiquement des applications** lorsque vous quittez momentanément son PC.

**2.6 Fermer ou verrouiller** la session quand l'ordinateur reste allumé et que vous vous absentez.

**2.7 Ne pas installer, télécharger ou utiliser** sur les matériels informatiques de l'établissement un logiciel sans licence d'utilisation appropriée ou inutile.

**2.8 S'interdire d'accéder** à des ressources informatiques pour lesquels vous ne bénéficiez pas d'une habilitation

**2.9 Avoir une obligation de confidentialité** à l'égard des informations et documents disponibles dans le système d'information.

**2.10 Utiliser les ressources** et les moyens informatiques prioritairement à des fins professionnelles.

**2.11 Respecter l'architecture réseau de l'établissement** en ne connectant pas d'éléments nouveaux. Pour toutes modifications ou extensions s'adresser au CETIAD.

## 3 Utilisez correctement la messagerie

**3.1 Cibler votre message :** L'objet doit refléter le contenu de votre message. Les spam et les virus envahissent nos boîtes aux lettres, et c'est souvent grâce au texte figurant dans l'objet que l'on peut faire un premier tri.

### 3.2:Soigner le contenu

Soyez prudent dans vos formulations : vos messages vous engagent. Etre bref et concis ne dispense pas d'être courtois.

**3.3 Envoyer une pièce jointe :** signaler la dans le corps de votre message pour éviter toute ambiguïté sur la nature de ce fichier (spam)

**3.4 Faire attention à la taille des fichiers** que vous envoyez. Un message trop lourd peut être rejeté par le serveur de messagerie.

**3.5 Vérifier le contenu et l'adresse des destinataires de votre mel!** Notamment lorsque vous répondez à un message d'une liste de diffusion, vérifier bien que l'adresse est celle de l'auteur (réponse en privé) ou l'adresse de la liste (l'ensemble des personnes inscrites).

**3.6 Penser que la sécurité sur Internet n'est jamais garantie :** L'envoi d'un mail peut être comparable à l'envoi d'une carte postale, il peut donc être lu par d'autres personnes.

**3.7 Etre bref :** plus votre message sera long, et moins il sera lu !!

**3.8 Donner toutes les citations,** références et sources et respectez les accords de Copyright...

**3.9 N'oublier pas que le mél n'est pas une messagerie instantanée.** N'attendez pas de réponse immédiate.

### Que faire pour prévenir l'infection

– ne pas activer l'ouverture automatique des pièces jointes

– Ne pas baser toute sa confiance sur des solutions techniques telles que l'antivirus, l'anti spam.

– Lorsque vous recevez une pièce jointe, vérifier que le contenu du message est en rapport avec ce document, si elle vous paraît suspecte ne pas cliquer dessus mais transférer le message pour analyse à l'adresse suivante. [spam@ac-dijon.fr](mailto:spam@ac-dijon.fr)

## 4 Protégez le réseau

### 4.1 Utiliser un pare-feu AMON

Le pare-feu AMON gère les communications dans le réseau de l'établissement. Il a aussi pour fonction le filtrage de sites et permet à l'établissement d'interdire l'accès à certains sites...

### 4.2 Utiliser un anti-virus

La solution académique installée sur un serveur de l'établissement et déployée sur les stations protège des attaques virales les serveurs et les PC du réseau. Cette solution se met à jour automatiquement sur internet.

Il est nécessaire pour rendre cette protection efficace que les systèmes (OS : windows, linux) utilisés sur les machines soient à jour. .

### 4.3 Charte

Elle précise de manière contractuelle les droits et devoirs de l'utilisateur et de l'établissement, fournisseur du service en rappelant notamment la législation liée à la protection de la vie privée et au respect de la propriété intellectuelle. Elle s'inscrit dans un objectif de sensibilisation et de responsabilisation.

<http://sicep.ac-dijon.fr/spip.php?article54>

## 5 Surveillez le réseau

**Utiliser les outils, mis à disposition, vous permettant de surveiller le fonctionnement du réseau.**

**EAD** sur le pare-feu AMON : sites visités

**Console de l'antivirus** : attaques virales

**Windows Update** pour les PC et les serveurs : mise à jour

**GDE** : gestion de parc administratif : état des PC

**ODR** : Outil de diagnostic du réseau.

## 6 Sauvegardez les données

### 6.1 Les menaces

**virus :** Ils se propagent instantanément et détruisent partiellement ou totalement les données stockées sur votre ordinateur.

**Spyware :** Il s'agit de programmes espions installés sans votre autorisation sur le pc lors de connexions internet. Ils espionnent votre comportement (adresses des sites que vous visitez, adresses de vos contacts sur votre messagerie, vos mots de passe, numéros de compte, votre profil d'utilisateur. Ils peuvent utiliser votre PC et votre connexion pour commettre des activités illicites en votre nom.

**Pannes du matériel :** Nul ne pourra vous aider à retrouver les données que vous aurez perdues lors de la panne!