Politique de Sécurité des Systèmes d'Information (PSSI)

Document d'orientation de la sécurité des systèmes d'information de l'Université de Poitiers.

1. Contexte et objectifs

1.1. Contexte

L'Université de Poitiers regroupe 7 unités de formation et de recherche, une école d'ingénieurs et 6 instituts qui accueillent actuellement 25000 étudiants dont 3000 étudiants internationaux de 110 nationalités. Cette diversité fait sa richesse et fonde sa capacité adaptative. L'ensemble des formations préparées à l'Université de Poitiers s'appuie sur une recherche d'excellence. Les recherches menées à l'Université de Poitiers couvrent un très large éventail de disciplines scientifiques. Cette spécificité multidisciplinaire permet d'encourager l'interdisciplinarité au travers notamment de grands programmes de recherche transversaux.

- 45 laboratoires
- 20 unités de recherche associées au CNRS
- 1 laboratoire propre (CNRS)
- 1 équipe associée à l'INSERM
- 21 équipes d'accueil (Université)
- structures fédératives de recherche
- 2 unités mixtes de services (CNRS - Université)
- 1 fédération reconnue par le CNRS
- 4 programmes pluri-formations
- 2 équipes de recherche technologiques
- 1 centre de recherche
- 870 enseignants chercheurs
- 103 chercheurs CNRS
- 120 chercheurs invités
- 1114 doctorants.

Implantée dans la capitale régionale, au centre-ville de Poitiers, sur le campus et sur l'aire de formation du Futuroscope, l'Université de Poitiers rayonne dans toute la région Poitou-Charentes avec des localisations à Châtellerault, Niort et Angoulême. La quinzaine de sites géographiques de l'Université de Poitiers est interconnectée au travers du réseau régional haut débit (SRHD), lui-même raccordé au Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche (Renater).

1.2. Périmètre de la SSI

La sécurité des systèmes d'information (SSI) de l'Université de Poitiers couvre l'ensemble des systèmes d'information de l'établissement avec toute la diversité que cela implique dans les usages, les lieux d'utilisation, les méthodes d'accès, les personnes concernées...

- le système informatique de gestion ;
- les applications institutionnelles (messagerie, applications et publications Internet, stockage, sauvegarde…) et celles propres aux composantes (applications scientifiques, traitement des données, bureautique…) ;
- les systèmes hors du champ informatique s'appuyant néanmoins sur ses ressources (ToIP/VoIP, visioconférence, vidéosurveillance, contrôle d'accès…) ;
- les interconnexions avec les autres organismes de tutelles (CNRS, INSERM).

1.3. Besoins de sécurité

La sécurité du Système d'Information repose sur les critères suivants :

- **Confidentialité** : « La confidentialité est la propriété qu'une information n'est ni disponible ni divulguée aux personnes, composantes ou processus non autorisés » norme ISO 7498-2 (ISO90).
- **Disponibilité** : Propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs autorisés.
- **Intégrité** : « L'intégrité est la prévention d'une modification non autorisée de l'information » norme ISO 7498-2 (ISO90).

Les besoins de sécurité s'appliquent aussi bien aux ressources du système d'information (postes informatiques, réseaux, applications…) qu'aux données traitées par ces ressources. Il est nécessaire d'inventorier et de classifier ces données (défense, scientifique, gestion, nominative, stratégique…) afin d'en identifier le degré de sensibilité et donc le besoin de protection nécessaire.

1.4. Menaces

Afin de mettre en place les moyens de sécurité adéquates, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité – DCSSI) préconise de connaître les typologies de menaces et leurs impacts. On distingue ainsi :

- les attaques visant directement le système d'information : vol de données (et éventuellement les ressources supportant ces données), modification des données, déni de service…
- les attaques visant les ressources informatiques : vol de ressources, détournement des ressources, altération des données, émission de malware…
- les accidents : sinistres naturels, altération accidentelle des données ou ressources…

Pour chaque menace, il est alors nécessaire d'en évaluer le risque, i.e. considérer la probabilité que celle-ci devienne réalité et détecter les éventuels facteurs aggravants (négligence constatée, insuffisance d'information, de consignes…).

1.5. Pilotage

Au sein de l'Université de Poitiers, la responsabilité générale de la sécurité des systèmes d'information relève du Président de l'université en tant qu'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI). Il est assisté dans cette fonction par le Responsable de la Sécurité des Systèmes d'Information (RSSI), également Fonctionnaire de Sécurité de Défense (FSD).

La PSSI de l'Université de Poitiers s'inscrit dans le cadre de la politique et des directives émanant de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), en charge de la sécurité des systèmes d'information au niveau national. Cette politique et ces directives sont relayées, pour ce qui est de la recherche, par le Haut Fonctionnaire de Défense et de Sécurité (HFDS) du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche et par le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) placé auprès de lui.

Le pilotage courant est de la responsabilité du RSSI et de son adjoint. La mise en œuvre opérationnelle est assurée par le RSSI et son adjoint pour le contrôle des données entrantes et sortantes ainsi que le service commun informatique et multimédia *i-médias* qui gère la chaine fonctionnelle des ressources institutionnelles. Les responsables hiérarchiques de composantes (directeurs, doyens…) sont responsables de la sécurité des systèmes d'information de leur

composante. Pour assurer cette fonction, ils nomment un correspondant SSI qui est le relais du RSSI au sein de sa composante tant pour appliquer et faire respecter la PSSI de l'établissement que pour lui remonter les éventuels incidents.

1.6. Coordination avec les autres tutelles

Les dispositions contractuelles qui régissent la tutelle de l'unité (contrat quadriennal) incluent celles relatives à la sécurité des systèmes d'information en définissant en particulier les responsabilités respectives. Ce document définit la PSSI de référence pour l'unité mixte ou l'unité propre. En tant que responsable de la SSI de son laboratoire, le directeur de l'unité :

- s'assure que les documents de PSSI de son unité (charte, gestion des traces…) sont en accord avec ceux de toutes ses tutelles (CNRS, EPST...) ;
- désigne le CSSI de son unité, celui-ci étant le « correspondant sécurité » pour les autres tutelles. Ce CSSI fait partie des chaînes fonctionnelles de chaque tutelle et assure les liens d'information correspondants.

En cas d'incident, celui-ci est traité par la voie fonctionnelle de la tutelle responsable, en assurant l'information des autres partenaires, avec si nécessaire une concertation sur les suites à donner telles que les dépôts de plainte.

2. Mise en œuvre de la PSSI à l'Université de Poitiers

La PSSI de l'Université de Poitiers affiche un ensemble de principes d'ordre organisationnel et technique à caractère prioritaire. Ces principes sont explicités, voire complétés, dans le cadre d'instructions ou dispositions techniques dont la responsabilité d'élaboration, de diffusion et d'information relève de la chaîne fonctionnelle SSI.

2.1 Organisation - Responsabilités

2.1.1. Responsabilité des différents acteurs

Les acteurs intervenant en matière de sécurité des systèmes d'information doivent être informés de leurs responsabilités en matière de SSI. Dans l'exercice de leur activité, ils sont liés à leur devoir de réserve voire à des obligations de secret professionnel.

Le Président de l'Université, le Secrétaire Général, le RSSI et son adjoint font l'objet d'une habilitation « confidentiel défense ».

2.1.2. Responsable de la Sécurité des Systèmes d'Information

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) exerce sous l'autorité directe du Président de l'Université de Poitiers, les activités suivantes :

- Contribuer activement à l'élaboration d'une politique de sécurité cohérente admise par tous et la mettre en œuvre.
- Viser tous les projets de l'établissement afin de veiller à la mise en œuvre au sein de ces derniers des éléments technologiques nécessaires à l'application de la PSSI.
- Coordonner, animer le réseau des correspondants sécurité de l'établissement.
- Exploiter et relayer les informations relatives à la sécurité en provenance du CERTA, du CERT-Renater, du CRU…
- Faire connaître et respecter la charte déontologique Renater ainsi que la charte d'utilisation des moyens informatiques et réseau de l'établissement.

- Proposer et mettre en œuvre des actions de sensibilisation et d'information de tous les utilisateurs aux aspects sécurité des systèmes d'information.
- Etre l'intermédiaire direct en cas de problème entre le Président de l'université et les autorités compétentes.

2.1.3. Accès aux ressources informatiques

La mise à disposition d'un utilisateur (personnel universitaire titulaire ou contractuel, CNRS, INSERM, étudiant) de moyens informatiques doit être formalisée à l'arrivée, au changement de fonction et au départ de l'intéressé. L'accès aux ressources doit être contrôlé (identification, authentification) et adapté au droit à en connaître de l'utilisateur (droits et privilèges, profil utilisateur).

2.1.4. Charte informatique

Préalablement à son accès aux outils informatiques, l'utilisateur doit prendre connaissance des droits et devoirs que lui confère la mise à disposition par sa composante de ces outils. Cette information se fait au travers de la « charte du bon usage des moyens informatiques » intégrée dans le règlement intérieur de l'Université de Poitiers.

2.1.5. Cyber surveillance

La sécurité des systèmes d'information exige de pouvoir surveiller le trafic sur le réseau et tracer les actions effectuées. Les dispositifs mis en œuvre doivent être conformes à la réglementation en vigueur et respecter les principes de proportionnalité (adaptation du niveau des moyens à l'enjeu effectif de la sécurité) et de transparence (information des partenaires sociaux et utilisateurs).

2.2. Protection des données

2.2.1. Disponibilité, confidentialité et intégrité des données

Le traitement et le stockage des données numériques, l'accès aux applications et services et les échanges de données entre systèmes d'information doivent être réalisés selon des méthodes visant à prévenir la perte, la modification et la mauvaise utilisation des données ou la divulgation des données ayant un caractère sensible.

Une sauvegarde régulière des données avec des processus de restauration régulièrement validés doit être mise en place. On distinguera les sauvegardes de production (par exemple, restauration d'une donnée) des sauvegardes de recours (par exemple, reprise des services sur des moyens externes suite à incident majeur). Une étude fine des données (criticité, volatilité, fluctuation…) permettra de définir la périodicité et le type de sauvegarde ainsi que la durée de rétention dans le respect des législations en vigueur.

2.2.2. Protection des données sensibles

Le stockage et la transmission de données « classifiées de défense » sont interdits sauf utilisation de moyens spécifiques agréés au niveau national. L'habilitation en elle-même ne suffit pas pour accéder à un document classifié. La seconde condition réside dans le besoin d'en connaître, c'est-à-dire la nécessité de prendre connaissance du document dans l'exercice de ses fonctions (cf. http://www.pleiade.education.fr/ - Communauté HFDS - Protection du secret et habilitation).

Les données non classifiées mais présentant un caractère sensible doivent être identifiées et le cas échéant repérées selon un niveau de sensibilité ; il sera procédé régulièrement à un réexamen de la sensibilité des données. Ces données devront faire l'objet d'une protection au niveau du contrôle d'accès (authentification et contrôle d'autorisation), du traitement, du stockage ou de l'échange (chiffrement) pour en assurer la confidentialité.

Avant toute cession ou mise au rebut d'un matériel ayant contenu des données sensibles, il est nécessaire de s'assurer que toutes les données ont bien été effacées par un procédé efficace et selon les recommandations techniques nationales. Si cela s'avère impossible les supports concernés devront être détruits.

2.2.3. Données à caractère personnel

Les traitements de données susceptibles de contenir des informations à caractère personnel (au sens de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) doivent faire l'objet des formalités requises de déclaration ou de demande d'autorisation auprès de la CNIL, via la correspondant CIL de l'établissement.

Les données à caractère personnel constituent des données sensibles et comme telles doivent faire l'objet de protection.

2.2.4. Chiffrement

Le chiffrement, en tant que moyen de protection, est obligatoire pour le stockage et l'échange de données sensibles. Les produits matériels et logiciels utilisés doivent faire l'objet d'un agrément par la DCSSI. Une copie des clés permettant de restituer les données en clair doit être stockée dans un lieu externe et sécurisé.

2.3. Sécurisation du Système d'information

2.3.1. Administration des serveurs

L'administration des serveurs de l'établissement est placée sous la responsabilité des administrateurs systèmes et réseaux du service commun informatique et multimédia *i-médias*. L'administration des serveurs des composantes est placée sous la responsabilité des administrateurs systèmes et réseaux de la composante.

2.3.2. Administration des postes de travail

L'administration des postes de travail individuels est placée sous la responsabilité des administrateurs systèmes et réseaux de la composante. L'administration des postes par les utilisateurs eux-mêmes doit demeurer l'exception et être justifiée en termes de besoins et de compétences. Les administrateurs systèmes et réseaux de l'établissement peuvent intervenir à distance pour des opérations de maintenance sur le poste de travail d'un utilisateur après l'en avoir averti et en respectant les principes de la loi Informatique et Libertés.

2.3.3. Sécurisation des postes de travail et des moyens nomades

La sécurisation des postes de travail et des moyens nomades est placée sous la responsabilité des administrateurs systèmes et réseaux de la composante. L'accès aux postes de travail et moyens nomades doit être protégé par mots de passe suffisamment robustes ; chaque mot de passe est personnel et confidentiel et, à ce titre, il ne doit pas être divulgué à un tiers, quel qu'il soit, ni laissé sans protection.

Les utilisateurs veillent au bon déroulement des applicatifs de sécurisation installés sur les moyens informatiques mis à leur disposition : mises à jour effectives de l'anti-virus, du système d'exploitation et des applications présentes, remontée des dysfonctionnements et incidents auprès du correspondant sécurité de leur composante… En particulier, les utilisateurs prendront des mesures spécifiques adaptées en cas d'utilisation des moyens nomades en dehors de leur zone de sécurité (protection contre le vol, chiffrement…).

2.3.4. Contrôle d'accès

Tout accès au système d'information est soumis à l'identification/authentification du demandeur et au contrôle de ses autorisations/habilitations. L'authentification doit se faire, dans la mesure du possible, au travers de l'annuaire SUPANN de l'établissement. Il importe de bien définir les autorisations et de n'attribuer que les privilèges nécessaires. Les accès doivent être journalisés. L'utilisation de comptes partagés ou anonymes doit demeurer l'exception et être justifiée en termes de besoins.

L'attribution et la modification des accès et privilèges d'un service doivent être validées par le propriétaire du service. Pour les services sensibles, un inventaire régulièrement mis à jour en sera dressé.

2.3.5. Sécurité des applications

La sécurité doit être prise en compte à toutes les étapes d'un projet, interne ou externe, lié au système d'information de l'établissement. Pour cela, un dossier de sécurité doit accompagner chaque projet et préciser les objectifs, les méthodes et les mesures préconisées. En particulier, les applications informatiques de gestion et les applications internet, doivent être sécurisées, en cohérence avec la sensibilité des informations traitées et échangées. Chaque dossier de sécurité doit être approuvée par le RSSI, voire le Président de l'Université de Poitiers (en tant qu'AQSSI) selon l'importance de l'application.

2.3.6. Infogérance et télémaintenance externes

L'infogérance correspond au fait que des sociétés extérieures, chargées de gérer une partie de l'informatique de l'établissement ou d'une composante, ont accès au système d'information depuis l'extérieur ou l'intérieur. Un contrat entre l'établissement et chaque société doit clairement préciser les droits d'accès, les engagements de responsabilités et l'imputabilité en cas d'incident. Des mécanismes permettant de s'assurer du respect des limites d'intervention doivent être mis en œuvre dans la mesure du possible.

L'externalisation de la gestion d'exploitation d'un composant critique pour le système d'information est à proscrire, sauf dispositions de garantie spécifiques et validées au niveau du RSSI , voire le Président de l'Université de Poitiers (en tant qu'AQSSI) selon l'importance de l'application.

2.3.7. Réseau

L'administration du réseau de l'établissement est placée exclusivement sous la responsabilité de la mission infrastructure réseau du service commun informatique et multimédia *i-médias*, et, sur les plaques géographiques distantes, par délégation aux administrateurs systèmes et réseaux des composantes concernées.

Les systèmes d'information doivent être protégés vis-à-vis de l'extérieur à l'aide de filtres d'accès appliqués sur les équipements en tête de son réseau. Ces filtres s'appliquent tant sur les flux réseau entrants que sur les flux sortants. Les flux entrants concernent principalement l'accès aux serveurs à partir du réseau de l'Université de Poitiers et/ou de l'extérieur ;

l'accès extérieur aux postes de travail doit demeurer l'exception et être justifiée en termes de besoins et de compétences. La politique de définition des filtres d'accès décrivant les flux réseau entrants est systématiquement du type « tout ce qui n'est pas explicitement autorisé est interdit ».

Les serveurs doivent être protégés spécifiquement vis-à-vis des postes de travail et des autres serveurs. On distinguera les serveurs accessibles uniquement à partir du réseau de l'Université de Poitiers et ceux accessibles aussi de l'extérieur. Pour chaque réseau de serveurs, les filtres d'accès, tant sur les flux réseau entrants que sur les flux sortants, sont systématiquement du type « tout ce qui n'est pas explicitement autorisé est interdit ». Les serveurs potentiellement accessibles de l'extérieur feront l'objet d'une surveillance accrue (outils d'analyse des trace, de métrologie…). L'accès externe aux serveurs par les moyens nomades de l'Université de Poitiers s'effectue au travers de connexions dédiées et chiffrées (VPN).

L'accès au réseau sans-fil doit faire l'objet d'un contrôle spécifique et n'être accessible qu'après authentification de l'utilisateur - personnes de l'Université de Poitiers ou du consortium UNR-PCL (Université de La Rochelle, Université de Limoges, ENSMA, ENSCI, CROUS). Les accès doivent être journalisés.

Une attention particulière doit être portée aux moyens nomades lors de leur réintroduction sur le réseau de l'Université de Poitiers pour éviter, notamment, de contaminer l'intérieur par des logiciels malveillants.

2.3.8. Maintien du niveau de sécurité

Le maintien du niveau de sécurité doit faire l'objet de dispositions techniques sous la responsabilité du RSSI. Ces dispositions doivent intégrer le maintien au cours du temps de l'état de sécurité des différents matériels : application des correctifs, mises à jour des anti-virus, pare-feu… Elles doivent préciser les conditions de surveillance du fonctionnement du système d'information de manière à s'assurer de son état de sécurité : analyse des journaux, vérification des vulnérabilités, suivi des avis de sécurité…

2.4. Mesure du niveau effectif de sécurité

2.4.1 Contrôle de gestion

Le contrôle de gestion de la sécurité des systèmes d'information s'opère sous la responsabilité du RSSI et du FSD. Il donne lieu à un tableau de bord de la SSI.

2.4.2. Audits

Le niveau de sécurité des systèmes d'information et la conformité de mise en œuvre des recommandations sur le terrain peuvent donner lieu à des audits internes sous la responsabilité du RSSI ou des audits externes sous la supervision du RSSI et après accord du Président de l'Université de Poitiers (en tant qu'AQSSI).

2.4.3. Journalisation, tableaux de bord

Le système d'information doit comprendre des dispositifs de journalisation centralisée et protégée de l'utilisation des services. L'objectif est de permettre de détecter des intrusions ou des utilisations frauduleuses, de tenter d'identifier les causes et les origines, d'éviter des contaminations d'autres sites par rebond et de remettre en place le système. Conformément à

la législation française, ces informations peuvent faire l'objet d'une transmission aux autorités compétentes après avis du Président de l'Université de Poitiers (en tant qu'AQSSI).

La durée de conservation des fichiers de traces à des fins de preuve doit être conforme aux lois et règlements en vigueur.

Il importe de définir, et de faire connaître aux utilisateurs, les règles d'exploitation des fichiers de traces (contenu, durée de conservation, utilisation) dans le respect du « principe de proportionnalité » et des contraintes législatives et réglementaires concernant notamment le traitement des informations à caractère personnel.

2.4.4. Les fichiers de traces

Les fichiers de traces seront systématiquement analysés afin de repérer d'éventuels problèmes et de produire des statistiques et tableaux de bord.

2.4.5. Posture de sécurité

En matière de sécurité des systèmes d'information, le niveau normal des recommandations faites dans le cadre de la politique interne de SSI correspond aux dispositions « jaune » et « orange » du plan Vigipirate. Ces recommandations sont rappelées régulièrement par le FSD.

Les dispositions internes de sécurisation doivent permettre une réactivité suffisante en cas de passage au niveau rouge de mesures propres à la SSI. Le plan d'intervention gouvernemental PIRANET fait l'objet annuellement d'exercices destinés à tester la réactivité de la chaîne d'intervention et la faisabilité des mesures préconisées.

2.4.6. Mises en garde

L'utilisation de certains matériels ou logiciels peut s'avérer préjudiciable à la sécurité des systèmes d'information. Ces produits font l'objet de « mises en garde » de la part de la chaîne fonctionnelle SSI (HFDS, FSD, RSSI…), visant soit des recommandations d'utilisation, soit une interdiction pure et simple.

2.4.7. Gestion d'incidents

Chaque acteur du système d'information, utilisateur ou administrateur, doit être sensibilisé à l'importance de signaler tout incident réel ou suspecté ; ceci inclut le vol de moyens informatiques ou de supports de données. Le signalement des incidents à la chaîne fonctionnelle SSI et aux autorités hiérarchiques est systématique.

Lorsque l'incident peut mettre en cause une composante ou l'Université de Poitiers dans son fonctionnement, le RSSI doit être informé directement, voire, parallèlement, le Président de l'Université de Poitiers (en tant qu'AQSSI) selon la gravité de l'incident (données sensibles…). Lorsque l'incident peut mettre en cause une composante classée ERR (Etablissements à Régime Restrictif), le RSSI, après avis du Président de l'Université de Poitiers (en tant qu'AQSSI), en informe les autorités compétentes (services du HFDS, DST…).

Toute infraction susceptible d'implications juridiques fera l'objet d'un dépôt de plainte par le RSSI auprès des autorités compétentes et après avis du Président de l'Université de Poitiers (en tant qu'AQSSI).

Dans le cas d'unités mixtes, il convient d'informer et le cas échéant de se concerter avec les autres tutelles.

Les données statistiques relatives à la gestion des incidents sont intégrées dans le tableau de bord de la SSI.

2.4.8. Gestion de crise

Le FSD prévoit le dispositif organisationnel propre aux crises de nature informatique ; il intègre les risques liés à l'informatique ainsi que les risques susceptibles d'une incidence sur la sécurité des systèmes d'information. Le FSD doivent être informés dès le déclenchement de toute crise ayant une incidence sur la sécurité des systèmes d'information. Il veille à la bonne information des autres structures concernées dont le RSSI, le Président de l'Université de Poitiers (en tant qu'AQSSI), les services du HFDS…

2.4.9. Plan de continuité

Chaque composante de l'Université de Poitiers doit définir un plan de continuité et les procédures correspondantes. Ce plan doit permettre, dans un premier temps, de maintenir en mode dégradé les activités critiques, puis de récupérer et de restaurer toutes les fonctionnalités du système d'information.

Dans le cas d'unités mixtes, il convient de se concerter avec les autres tutelles.

Charte du bon usage des moyens informatiques de l'Université de Poitiers

1. Objet

La présente charte a pour objet de définir les conditions d'utilisation et les règles de bon usage des moyens informatiques de l'Université de Poitiers et d'assurer le développement de l'utilisation de l'informatique dans le respect des lois et règlements.

2. Domaine d'application

La charte s'applique à l'ensemble des personnes qui, quel que soit leur statut, ont accès aux moyens informatiques de l'Université de Poitiers.

3. Moyens informatiques

Sont **notamment** constitutifs de moyens informatiques, les serveurs, stations de travail, postes de consultation, les réseaux internes et externes de l'Université de Poitiers, les micro-ordinateurs des services, laboratoires, instituts, centres, facultés, ainsi que l'ensemble du parc logiciel, des bases de données, des produits multimédias ou des périphériques affectés au fonctionnement des éléments décrits. Sont également considérés comme moyens informatiques, les ressources extérieures accessibles par l'intermédiaire des réseaux de l'Université de Poitiers et notamment le réseau RENATER.

4. Utilisations

4.1 Finalité de l'utilisation des moyens informatiques de l'Université de Poitiers

L'utilisation des moyens informatiques est limitée au strict cadre et aux seuls besoins de l'activité et de la vie universitaire.

4.2 Autorisations particulières

Toute autre utilisation des moyens informatiques de l'Université de Poitiers doit être préalablement autorisée par le Président de l'Université ou son représentant.

4.3 Utilisations prohibées

Sont strictement prohibées les utilisations contraires aux lois et règlements en vigueur et notamment celles qui ont pour objet ou pour effet, la diffusion d'idéologies politiques, ou qui sont de nature à porter atteinte aux bonnes mœurs, à la dignité, à l'honneur, ou à la vie privée des personnes.

5. Utilisateurs

5.1 Identification des utilisateurs

Par utilisateur, on entend toute personne qui, à titre habituel ou non, professionnel ou non, est autorisée à accéder aux moyens informatiques de l'Université de Poitiers.

5.2 Obligations des utilisateurs

5.2.1 Règles générales

Les utilisateurs sont tenus de respecter la charte des bons usages de l'informatique de l'Université de Poitiers. Les utilisateurs doivent respecter les lois et règlements en vigueur ainsi que les règles de courtoisie et de politesse lors de l'utilisation des moyens informatiques de l'Université de Poitiers. Les utilisateurs doivent faire une utilisation non-abusive des moyens informatiques auxquels ils ont accès.

Les utilisateurs doivent respecter les mesures de sécurité des moyens informatiques prévues à l'article 8 de la présente charte. Les utilisateurs sont tenus de se conformer aux décisions des responsables informatiques.

5.2.2 Fichiers des utilisateurs

Les utilisateurs peuvent créer des fichiers privés pour lesquels ils ont le droit d'accès exclusif. Ces fichiers doivent être considérés comme privés tant que leur créateur ne les a pas mis à la disposition du public. Sont interdites la destruction, l'altération ou la reproduction d'un fichier mis à la disposition du public, en dehors des cas où elles sont expressément autorisées.

5.2.3 Préservation des matériels et locaux

Les utilisateurs sont tenus de respecter les matériels, logiciels et locaux mis à leur disposition. Les utilisateurs qui constatent une dégradation ou un dysfonctionnement doivent, dans les plus brefs délais, informer le responsable informatique.

5.2.4 Pénétration non autorisée dans les moyens informatiques

La pénétration non autorisée et le maintien dans un moyen informatique par un utilisateur sont interdits. Les utilisateurs ne doivent pas utiliser ou tenter d'utiliser le compte d'un tiers. Est également interdite toute manœuvre qui viserait à accéder aux moyens informatiques sous une fausse identité ou en masquant l'identité véritable de l'utilisateur.

5.2.5 Utilisation des comptes et des dispositifs de contrôle d'accès

Les utilisateurs doivent prendre toutes mesures pour limiter les accès frauduleux aux moyens informatiques, à ce titre ils doivent **notamment** :

- veiller à la confidentialité des codes, mots de passe, cartes magnétiques, clefs ou tout autre dispositif de contrôle d'accès qui leur sont confiés à titre strictement personnel ;
- veiller à la confidentialité des comptes utilisateurs qui leur sont attribués à titre strictement personnel ;
- ne pas prêter, vendre ou céder les comptes utilisateurs, codes et autres dispositifs de contrôle d'accès ou en faire bénéficier un tiers ;
- se déconnecter immédiatement après la fin de leur période de travail sur le réseau ou lorsqu'ils s'absentent ;
- informer immédiatement le responsable informatique et le Responsable de la Sécurité des Systèmes d'Information (RSSI) de toute tentative d'accès frauduleux ou de tout dysfonctionnement suspect ;
- changer régulièrement les codes d'accès ;
- s'assurer que les fichiers qu'ils jugent confidentiels ne soient pas accessibles à des tiers ;
- informer le responsable informatique et le Responsable de la Sécurité des Systèmes d'Information (RSSI) des périodes durant lesquelles ils n'utiliseront pas leurs comptes.

5.3 Responsabilité des utilisateurs

5.3.1 Responsabilité des utilisations

Les utilisateurs sont responsables de l'utilisation qu'ils font des moyens informatiques de l'Université de Poitiers ainsi que de l'ensemble des informations qu'ils mettent à la disposition du public.

5.3.2 Responsabilité des comptes et dispositifs de contrôle d'accès

Les titulaires de comptes, ou d'un dispositif de contrôle d'accès, sont responsables des opérations locales ou distantes effectuées depuis leurs comptes ou sous le couvert des dispositifs de contrôle d'accès qui leur ont été attribués.

5.4 Sanctions

En cas de non respect de leurs obligations, les utilisateurs peuvent se voir appliquer les sanctions prévues à l'article 9.

6. Responsables informatiques

6.1 Nomination

Les directeurs de services, laboratoires, instituts, centres, facultés nomment pour chaque site informatique placé sous leur autorité, un ou plusieurs responsables ci-après désignés responsables informatiques.

6.2 Fonction des responsables informatiques

Les responsables informatiques :

- autorisent les accès aux moyens informatiques ;
- attribuent les comptes et les mots de passe, cartes magnétiques, clefs ou tout autre dispositif permettant de limiter l'accès aux moyens informatiques conformément aux instructions du directeur ;
- définissent les utilisations conformes à la vocation des moyens informatiques mis à la disposition des utilisateurs, sous le contrôle de l'équipe pédagogique ou du directeur ;
- informent les utilisateurs des bons usages tels qu'ils sont définis dans la présente charte ;
- assurent le fonctionnement et la disponibilité normale des moyens informatiques.

6.3 Pouvoir des responsables informatiques

Les responsables informatiques peuvent surveiller les utilisations qui sont faites des moyens informatiques dont ils ont la charge. Dans le cadre de leurs fonctions, les responsables informatiques peuvent prendre connaissance des fichiers, des données et des travaux des utilisateurs ainsi que des ressources extérieures qu'ils utilisent. Les responsables informatiques peuvent, en cas d'urgence, prendre toutes les mesures nécessaires pour assurer ou préserver le bon fonctionnement et la disponibilité normale des moyens informatiques qui leur sont confiés.

6.4 Obligations des responsables informatiques

6.4.1 Confidentialité

Les responsables informatiques doivent préserver la confidentialité des informations et des fichiers auxquels ils ont accès dans le cadre de leurs fonctions.

6.4.2 Qualité du service

Les responsables informatiques doivent s'efforcer de limiter la gêne occasionnée aux utilisateurs par leurs interventions sur les moyens informatiques de l'Université de Poitiers. Les responsables informatiques doivent s'efforcer d'assurer une disponibilité normale et le bon fonctionnement des moyens informatiques.

6.4.3 Information

Les responsables informatiques sont tenus d'informer le Responsable de la Sécurité des Systèmes d'Information (RSSI) et le directeur du Centre de Ressources Informatiques de l'Université de Poitiers (CRIUP) de toute violation ou tentative de violation d'accès ou de tout autre élément de nature à mettre en péril la sécurité des moyens informatiques de l'Université de Poitiers.

6.4.4 Sécurité

Les responsables informatiques doivent s'assurer que les codes d'accès choisi par les utilisateurs répondent aux exigences de sécurité telles qu'elles sont édictées par le Centre de Ressources Informatiques de l'Université de Poitiers (CRIUP) et le Responsable de la Sécurité des Systèmes d'Information (RSSI).

7. Données nominatives

Les traitements automatisés de données nominatives mis en œuvre par l'Université, ses composantes ou par tout utilisateur doivent respecter les dispositions de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

8. Modification et altération des moyens informatiques

8.1 Modification des environnements

En dehors des modifications ne portant pas atteinte au bon fonctionnement des moyens informatiques, aucune modification des environnements logiciels, matériels et périphériques ne pourra être effectuée sans l'accord préalable du responsable informatique. Par modification d'environnement, on entend toute suppression ou ajout de composants logiciels ou matériels ou tout paramétrage pouvant affecter le fonctionnement normal des moyens informatiques.

8.2 Virus, chevaux de Troie, bombes logiques

L'introduction, l'utilisation, la diffusion de tout dispositif logiciel ou matériel qui pourrait altérer les fonctionnalités des moyens informatiques sont interdites. Les recherches portant sur les virus, chevaux de Troie, bombes logiques et autres dispositifs qui pourraient altérer les fonctionnalités des moyens informatiques doivent être préalablement autorisées par le responsable informatique.

9. Conséquences des manquements à la charte et poursuites

9.1 Mesures et sanctions applicables par les responsables informatiques

9.1.1 Mesures d'urgence

Les responsables informatiques peuvent en cas d'urgence :

- déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;
- isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques.

9.1.2 Mesures donnant lieu à information

Sous réserve que soit informé le directeur ou le responsable du service, les responsables informatiques peuvent :

- avertir un utilisateur ;
- limiter provisoirement les accès d'un utilisateur ;
- à titre provisoire, retirer les codes d'accès et fermer les comptes ;
- effacer, comprimer ou isoler toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques ;
- informer le Responsable de la Sécurité des Systèmes d'Information (RSSI) ;
- informer le Président de l'Université.

9.1.3 Mesures soumises à autorisation du directeur ou responsable du service

Sous condition d'autorisation préalable du directeur ou du responsable de service, les responsables informatiques peuvent :

- retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes ;
- interdire à titre définitif à un utilisateur tout accès aux moyens informatiques dont il est responsable.

9.2 Autres sanctions internes

Sans préjudice du pouvoir de sanction des centres, instituts, UFR et autres composantes de l'Université de Poitiers, le Président de l'Université peut prendre toutes les sanctions internes qui permettraient d'assurer le respect de la charte et le bon fonctionnement de l'université ou de ses services. **En particulier,** des sanctions disciplinaires peuvent être prises, dans le cadre du décret n° 92-657 du 13 juillet 1992 relatif à la procédure disciplinaire dans les établissements publics d'enseignement supérieur. Les sanctions internes ou disciplinaires ne sont pas exclusives de poursuites civiles ou pénales.

9.3 Poursuites civiles et pénales

Le Président peut, après avis du Conseil d'Administration de l'Université, engager des poursuites civiles à l'encontre des utilisateurs. Le Président peut, après avis du Conseil d'Administration de l'Université, informer le Procureur de la République des infractions commises par les utilisateurs.