UNIVERSITÉ TOULOUSE 1 CAPITOLE

RESULTAT DU VOTE
Nombre de votants : 21
Voix favorables : 21
Voix défavorables : 0
Abstention : 0

CONSEIL D'ADMINISTRATION
Séance du 12/04/2022

DELIBERATION
n° **CA 2022 - 32**

portant approbation de la révision des statuts de l'Institut Universitaire et Technologique de Rodez - IUT

Vu le code de l'éducation, notamment son article L. 712-3,

Vu l'avis du Comité Technique de l'Université Toulouse 1 Capitole dans sa séance du mardi 8 février 2022,

Vu l'avis du Conseil de l'IUT de Rodez dans sa séance du lundi 7mars 2022,

Le conseil d'administration, après en avoir délibéré, décide :

Article unique

Le conseil d'administration approuve la révision des statuts de l'Institut Universitaire et Technologique de Rodez - IUT annexés à la présente délibération.

Le président du conseil d'administration,

UNIVERSITÉ TOULOUSE 1 CAPITOLE

Hugues KENFACK

STATUTS

Date de dernière mise à jour : 14/02/2022 – 8h
VERSION DEFINITIVE après CT du 8 février 2022

INSTITUT UNIVERSITAIRE DE TECHNOLOGIE DE RODEZ

Approuvés par le Conseil d'Administration du 27 mars 1990
Modifiés par le Conseil d'Administration du 24 novembre 2003
Modifiés par le Conseil d'Administration du 15 décembre 2008
Modifiés par le Conseil d'Administration du 7 février 2011
Modifiés par le Conseil d'Administration du 12 avril 2022

SOMMAIRE

TITRE 1 –Dispositions générales, Missions, Structures

Article 1 - Désignation

L'Institut Universitaire de Technologie de Rodez, créé par le décret n° 87-421 du 12/06/1987 est un Institut de l'Université Toulouse 1 Capitole au sens des articles L. 713-1 du Code de l'Education. Il est organisé dans les conditions définies aux articles L. 713-9 et D. 713-1 et suivants du Code de l'Education.

Article 2 - Missions

L'IUT de Rodez a pour missions :

- de dispenser un enseignement supérieur technologique et général, en formation initiale et continue tout au long de la vie,
- de contribuer à la recherche scientifique universitaire en collaboration avec d'autres établissements universitaires et organismes publics ou privés. Il participe à la diffusion de la culture et de l'information scientifique et technique,
- de concourir au développement des relations internationales,
- de participer à la création et au fonctionnement de toute filière technologique.

Article 3 - Structures

L'IUT de Rodez est administré par un Conseil et dirigé par un Directeur.
Il est organisé en départements pédagogiques correspondants aux grandes spécialités qui y sont enseignées :

- Gestion des Entreprises et des Administrations,
- Informatique,
- Qualité, Logistique Industrielle et Organisation,
- Information – Communication,
- Carrières Juridique.

TITRE 2 – Le Conseil de l'IUT

Article 4 - Rôle et compétences

Le Conseil a notamment pour compétences :

- d'établir la politique générale de l'IUT,
- de modifier les statuts,
- d'élaborer et modifier, si nécessaire, le règlement intérieur,
- de se prononcer sur les adaptations locales aux programmes d'enseignements nationaux, proposées par les départements,
- d'adopter le budget de l'IUT proposé par le Directeur et approuvé par le Conseil d'administration de l'Université. Il approuve l'exécution du budget,
- de se prononcer sur les moyens matériels et humains de l'IUT de Rodez,
- de donner son avis sur les contrats et conventions dont l'exécution le concerne,
- de procéder à l'élection du Directeur selon les modalités prévues à l'article 10 des présents statuts,
- de donner son avis pour la nomination des Chefs de Départements par le Directeur selon les modalités prévues à l'article 15 des présents statuts,
- d'être informé par les Chefs de Départements et le Directeur, des principes de la pédagogie et du contrôle des connaissances,
- de créer toute commission temporaire ou permanente utile au fonctionnement de l'IUT,
- de prendre toute initiative dans l'intérêt de l'IUT.

Article 5 - Composition

Le Conseil de l'IUT comprend 36 membres :

- **12 représentants des enseignants et chargés d'enseignement comportant :**

  - 6 représentants des enseignants-chercheurs et assimilés :
    - 1 représentant des Professeurs d'Université en poste à l'IUT ou à défaut y dispensant des enseignements,
    - 5 représentants des autres enseignants-chercheurs et assimilés,
  - 5 représentants des autres enseignants,
  - 1 représentant des chargés d'enseignement.

- **4 représentants du personnel BIATSS**

- **8 représentants des usagers :**
  Pour chaque représentant, un suppléant est élu dans les mêmes conditions que le titulaire.

- **12 personnalités extérieures :**

  - 1 représentant du Conseil Régional d'Occitanie,
  - 1 représentant du Conseil Départemental de l'Aveyron,
  - 1 représentant de Rodez agglomération,
  - 5 représentants des activités professionnelles auxquelles prépare l'IUT,
  - 4 personnalités désignées à titre personnel, en raison de leur compétence et, notamment, leur rôle dans les activités correspondant aux spécialités enseignées à l'IUT, de l'intérêt qu'elles portent à l'activité de l'IUT de Rodez.

Le Président de l'Université Toulouse 1 Capitole ou son représentant, le Directeur de l'IUT, le Responsable administratif et financier, le(s) Directeur(s) Adjoint(s) et les Chefs de Département, quand ils ne sont pas membres élus du Conseil, assistent de droit aux réunions avec voix consultative.

Article 6 - Désignation

Article 6.1 Représentants des enseignants

En application de l'article D713-1 du code de l'éducation, l'élection des représentants des personnels enseignants en activité à l'IUT s'effectue par collèges distincts :

- Professeurs des universités et assimilés ;
- Autres enseignants-chercheurs et assimilés ;
- Autres enseignants ;
- Chargés d'enseignement.

Pour être inscrits sur les listes électorales du collège correspondant à leur catégorie, les personnels enseignants doivent remplir les conditions précisées à l'article D719-9 du Code de l'Education.

Article 6.2 Représentants des personnels des bibliothèques, ingénieurs, administratifs, techniques, sociaux et de santé (BIATSS)

Les électeurs sont regroupés en un seul collège qui comprend les personnels BIATSS affectés à l'IUT. Il comprend également les membres des corps des ingénieurs et personnels techniques et administratifs de recherche et de formation.

Article 6.3 Représentants des usagers

Le collège comprend les étudiants régulièrement inscrits à l'IUT, ainsi que les personnes bénéficiant de la formation continue et les auditeurs, dans les conditions prévues à l'article D. 719-14 du Code de l'Education.

Article 6.4 Personnalités extérieures

Leur mandat est de trois ans.
La liste des cinq institutions et organismes, publics ou privés, appelés à être représentés au conseil de l'institut au titre des activités professionnelles auxquelles prépare l'IUT est fixée par délibération prise à la majorité des deux tiers des membres en exercice, élus et nommés, du conseil. Elle peut être modifiée, avant chaque renouvellement, dans les mêmes formes.. Lorsque cette liste comporte des représentants d'organisations syndicales, les représentants des organisation syndicales d'employeurs et de salariés sont en nombre égal.
La parité entre les femmes et les hommes est assurée parmi les personnalités extérieures siégeant au Conseil.
Les personnalités siégeant à titre personnel sont désignées suite à un appel à candidatures publié sur le site internet de l'IUT au moins quinze jours avant la séance. Leur désignation est acquise par un vote à la majorité absolue des membres en exercice, élus et nommés, du conseil.
Le choix final des personnalités siégeant à titre personnel tient compte de la répartition par sexe des personnalités extérieures désignées par les collectivités territoriales, institutions et organismes appelés à nommer leurs représentants. Si la parité n'a pu être établie, un tirage au sort détermine qui, parmi ces collectivités, institutions et organismes ayant désigné un représentant du sexe surreprésenté, est ou sont appelés à désigner une personnalité du sexe sous-représenté.

Article 6.5 Mandats

Le mode et le déroulement du scrutin sont ceux définis aux articles D. 719-1 et suivants du Code de l'Education.

En vertu de l'article L 719-1 du Code de l'Education, le renouvellement des mandats intervient tous les quatre ans pour tous les collèges, sauf pour les collèges étudiants où le renouvellement intervient tous les deux ans et les personnalités extérieures tous les trois ans.

Lorsqu'une personnalité extérieure perd la qualité au titre de laquelle elle avait été désignée, ou cesse définitivement de siéger pour quelque cause que ce soit, un représentant du même sexe est désigné pour la durée du mandat restant à courir..

Lorsqu'un représentant des personnels perd la qualité au titre de laquelle il a été élu ou lorsque son siège devient vacant, il est remplacé, pour la durée du mandat restant à courir, par le candidat de la même liste venant immédiatement après le dernier candidat élu. En cas d'impossibilité, il est procédé à un renouvellement partiel.

Lorsqu'un représentant titulaire des usagers perd la qualité au titre de laquelle il a été élu ou lorsque son siège devient vacant, il est remplacé, pour la durée du mandat restant à courir, par son suppléant qui devient titulaire. Lorsque le siège d'un représentant suppléant devient vacant pour quelque cause que ce soit, il est attribué, pour la durée du mandat restant à courir, au premier des candidats non élu de la même liste. Lorsque le siège vacant d'un représentant titulaire ne peut plus être pourvu dans l'ordre de présentation de la liste par application des dispositions prévues au présent alinéa, il est procédé à un renouvellement partiel.

Conformément à l'article L 713-9 du Code de l'Education, le Conseil élit un Président parmi les personnalités extérieures, pour un mandat de trois ans renouvelable.

Article 7 - Le Président et le Vice-président du Conseil de l'IUT

Article 7-1. Election du Président et du Vice-président

Le Conseil de l'IUT élit à la majorité, pour un mandat de trois ans, au sein des personnalités extérieures, celui de ses membres qui est appelé à le présider. Le mandat du Président est renouvelable (L 713-9 alinéa 2 du Code de l'Education).
En cas d'interruption du mandat du Président, son successeur est élu pour la durée du mandat restant à courir.

Le Conseil élit dans les mêmes conditions un Vice-président au sein des personnalités extérieures.

Article 7-2. Attributions du Président du Conseil

Les compétences du Président sont, en particulier, les suivantes :

- Il convoque le Conseil et arrête l'ordre du jour,
- Il a accès à tous les renseignements et documents nécessaires à la préparation des délibérations du Conseil et au suivi de leur exécution,
- Il veille à la conformité des décisions du Conseil avec la législation et la réglementation en vigueur,
- Il représente l'IUT auprès des milieux socioprofessionnels.

Article 7-3. Attributions du Vice-président du Conseil

Le vice-président supplée le Président du Conseil en cas de nécessité.
En cas de démission ou d'incapacité permanente du Président du Conseil à remplir ses fonctions, le vice-président est appelé à assurer l'intérim jusqu'au conseil suivant.
Le vice-président exerce les attributions définies à l'article 7-2.

Article 8 - Fonctionnement du Conseil

Le Conseil se réunit au minimum 3 fois par an en session ordinaire sur convocation de son Président. Le Conseil peut également se réunir en séance extraordinaire, sur convocation de son Président, à son initiative, à la demande du Directeur ou du tiers de ses membres.

La convocation doit être envoyée aux membres du Conseil au moins une semaine avant la réunion, sauf situation d'urgence. Elle doit être accompagnée de l'ordre du jour et, le cas échéant, des documents nécessaires à la compréhension et à l'étude des différents points de l'ordre du jour.

Les séances du Conseil sont présidées par le Président ou, en cas d'empêchement de celui-ci, par le vice-président.

Sur décision du Conseil, de son Président ou du Directeur, des personnes extérieures au Conseil peuvent être invitées à participer aux séances à titre consultatif.

Délibérations du Conseil

Le Conseil délibère valablement lorsque au moins la moitié de ses membres sont présents ou représentés par procuration écrite. Nul membre du Conseil ne peut détenir plus de deux procurations.

Si ce quorum n'est pas atteint, le Conseil est convoqué dans un délai de 15 jours sur les points initialement prévus à l'ordre du jour et dans ce cas, aucun quorum n'est exigé.

Les décisions sont prises à la majorité des suffrages exprimés, sauf en ce qui concerne l'adoption ou la révision des statuts, où la majorité des deux tiers des membres en exercice est requise.

Le vote peut avoir lieu à main levée, sauf si une objection est faite par un membre du Conseil ; le vote a alors lieu à bulletin secret. Lorsqu'il est question de personnes nommément désignées, le vote a toujours lieu à bulletin secret.

Compte-rendu des séances

Le compte-rendu est soumis à l'approbation du Conseil au début de la séance suivante. Les demandes de modification sont soumises au vote.

Avant approbation par le Conseil, les comptes rendus des séances sont adressés aux membres du Conseil.
Après approbation, les comptes rendus sont rendus accessibles au personnel de l'IUT.

Article 9 – Le Conseil restreint

Le Conseil de l'IUT, réuni en formation restreinte aux élus enseignants-chercheurs, est consulté sur les décisions individuelles d'attribution de services des enseignants-chercheurs.

TITRE 3 - Le Directeur

Article 10 - Mandat

Le Directeur est élu à la majorité absolue des membres composant le Conseil, dans l'une des catégories de personnel qui ont vocation à enseigner dans les IUT (articles L 713-9 et D. 713-1 du Code de l'Education).

Son mandat est de 5 ans immédiatement renouvelable une fois.

Article 11 - Attributions

Le Directeur a notamment pour attributions :

- de diriger et de représenter l'Institut,
- de préparer les travaux du Conseil, en liaison avec le Président du Conseil et le Comité directeur,
- de mettre en œuvre les décisions du Conseil et de lui en rendre compte,
- de proposer au Conseil le budget de l'IUT,
- d'être ordonnateur des recettes et des dépenses dans le cadre du budget propre de l'IUT,
- de procéder au choix des personnels suivant la réglementation en vigueur,
- d'avoir autorité sur l'ensemble des personnels de l'IUT de Rodez. Aucune affectation ne peut être prononcée si le Directeur de l'IUT émet un avis défavorable motivé,
- de nommer les Chefs de Département et les Responsables pédagogiques de formation L3,
- de désigner un ou plusieurs Directeurs Adjoints.

Article 12 – Le comité directeur

- Sa composition. Il est composé :
  - du Directeur et de(s) Directeur(s) Adjoint(s),
  - des Chefs de Département,
  - du Responsable administratif et financier,
  - d'un représentant du personnel BIATSS élu au Conseil de l'IUT, désigné par les représentants BIATSS élus au Conseil de l'IUT,
  - de toute personne dont la présence est jugée nécessaire en fonction de l'ordre du jour.

- Ses attributions :
  - veiller avec le Directeur à l'exécution des décisions prises par le Conseil,
  - préparer avec le Directeur et le Président du Conseil les travaux du Conseil,
  - assister le Directeur pour toutes les décisions importantes à prendre dans l'intervalle des réunions du Conseil.

Il rend accessible au moins aux Chefs de Département et de service, les comptes rendus du comité.
Il est présidé par le Directeur ou le Directeur Adjoint en cas d'empêchement.

Article 13 – Le/les Directeurs Adjoints

Le Directeur de l'IUT peut nommer après approbation du Conseil un ou des Directeurs Adjoints, choisi parmi les personnels ayant vocation à enseigner dans l'IUT.

Le Directeur fixe les attributions du Directeur Adjoint. Le Directeur Adjoint peut assister et représenter le Directeur dans tous les conseils et commissions.

Le mandat du Directeur Adjoint prend fin avec celui du Directeur. Le Directeur peut mettre fin aux fonctions du Directeur Adjoint avant la fin de ce mandat. Il en informe le Conseil de l'IUT.

TITRE 4 - Les Départements

Article 14 – Les Départements

Conformément à l'article D. 713-3 du Code de l'Education, l'IUT comprend des départements correspondant aux spécialités enseignées. Chaque département est dirigé sous l'autorité du Directeur de l'IUT par un Chef de Département assisté d'un Conseil de Département.

Article 15 - Le Chef de Département

Article 15.1 Nomination

Le Chef de Département est nommé par le Directeur de l'IUT après avis favorable du Conseil de l'IUT et consultation préalable du Conseil de Département.
Peut être nommé Chef de Département toute personne ayant vocation à enseigner dans le département.
La nomination du Chef de Département est prononcée pour une durée de 3 ans immédiatement renouvelable une fois.

Dans l'hypothèse où aucun enseignant n'est candidat au titre de Chef de Département, le Directeur de l'IUT désigne un administrateur provisoire, dans l'attente de la désignation du nouveau Chef de Département.

Article 15.2 Attributions

Le Chef de Département a notamment pour attributions :

- de représenter le département,
- de diriger le département en accord avec le Conseil de Département,
- de préparer les travaux du Conseil de Département,
- d'informer le Conseil de Département des décisions du Conseil de l'IUT. En accord avec le Conseil de Département, il met en œuvre les décisions qui lui sont transmises par le Directeur de l'IUT,
- de coordonner l'ensemble des activités pédagogiques, administratives et techniques du département.

Article 16 - Le Conseil de Département

Article 16.1 Rôle

Le Conseil de Département assiste le Chef de Département pour la coordination des activités pédagogiques, administratives et techniques du département, en accord avec les textes en vigueur et les décisions du Conseil de l'IUT.
Il est consulté en vue de la nomination du Chef de Département. Dans ce dernier cas, la réunion est convoquée et présidée par le Directeur de l'IUT de Rodez.

Article 16.2 Composition

En début d'année universitaire, le Chef de Département met à jour et rend publique la liste des membres du Conseil de Département qui devra comprendre :

- les enseignants-chercheurs effectuant au moins 64 heures équivalent TD dans les formations assurées par le département
- les autres enseignants titulaires effectuant au moins 128 heures équivalent TD dans les formations assurées par le département
- les maîtres de conférences associés ("PAST") effectuant au moins 48 heures équivalent TD dans les formations assurées par le département
- les chargés d'enseignement vacataires effectuant au moins 48 heures équivalent TD dans les formations assurées par le département
- les enseignants contractuels effectuant au moins la moitié de leur engagement contractuel dans les formations assurées par le département
- les représentants étudiants
- les personnels BIATSS affectés à des formations assurées par le département

Les représentants des étudiants sont élus pour un an dans chaque département à raison d'un délégué par groupe de travaux dirigés, selon le mode de scrutin en vigueur pour l'élection des étudiants au Conseil de l'IUT. L'élection a lieu au plus tard le 31 octobre de l'année universitaire.

Article 17 – Le Conseil de perfectionnement

Article 17.1 Rôle

Dans une logique d'amélioration continue, le Conseil de perfectionnement examine une fois par an les indicateurs du Bachelor Universitaire de Technologie de la spécialité, notamment les résultats des évaluations des formations et des enseignements par les étudiants, les suivis de cohortes, la qualité des stages et le suivi de l'insertion professionnelle.
Le Conseil de l'IUT est ensuite informé de l'ensemble des évaluations internes des départements.

Un Conseil de perfectionnement est créé dans chaque département de formation.

Article 17.2 Composition

En début d'année universitaire, le Chef de Département met à jour et rend publique la liste des membres du Conseil de perfectionnement qui devra comprendre :

- des enseignants chercheurs,
- des enseignants,
- des personnels BIATSS affectés à des formations assurées par le département,
- des représentants du monde socio-professionnel,
- des étudiants.

TITRE 5 – Dispositions finales

Article 18 – Entrée en vigueur

Les dispositions des articles 5, 6.4 et du 3ème alinéa de l'article 6.5 des présents statuts entrent en vigueur en vue du prochain renouvellement complet des représentants des personnels et des usagers du conseil de l'IUT. Le mandat des personnalités extérieures en cours à la date de ce renouvellement prend fin en même temps que le mandat des représentants des personnels et des usagers appelés à être renouvelés.

UNIVERSITÉ TOULOUSE 1 CAPITOLE

RESULTAT DU VOTE
Nombre de votants : 21
Voix favorables : 21
Voix défavorables : 0
Abstention : 0

CONSEIL D'ADMINISTRATION
Séance du 12/04/2022

DELIBERATION
CA n° 2022 - 32

portant approbation de la révision du règlement intérieur de l'Institut Universitaire et Technologique de Rodez - IUT

Vu le code de l'éducation, notamment son article L. 712-3,

Vu l'avis du Comité Technique de l'Université Toulouse 1 Capitole dans sa séance du mardi 8 février 2022,

Vu l'avis du Conseil de l'IUT de Rodez dans sa séance du lundi 7 mars 2022,

Vu l'avis du Comité d'Hygiène, de Sécurité et des Conditions de Travail dans sa séance du 10 mars 2022,

Vu l'avis de la Commission de la Formation de la Vie Universitaire dans sa séance du mardi 22 mars 2022,

Le conseil d'administration, après en avoir délibéré, décide :

Article unique

Le conseil d'administration approuve la révision du règlement intérieur de l'Institut Universitaire et Technologique de Rodez- IUT annexé à la présente délibération.

Le président du conseil d'administration,

UNIVERSITÉ TOULOUSE 1 CAPITOLE

Hugues KENFACK

RÈGLEMENT INTÉRIEUR

Date de dernière mise à jour : 14/02/2021 – 8 h
VERSION DEFINITIVE après CT du 8 février 2022

INSTITUT UNIVERSITAIRE DE TECHNOLOGIE DE RODEZ

Le directeur de l'IUT de Rodez est responsable de l'exécution du présent règlement intérieur

TITRE I –Dispositions générales

Article 1. Objectifs du règlement intérieur

L'Institut Universitaire de Technologie de Rodez est une composante de l'Université Toulouse 1 Capitole au sens de l'article L.713-9 du code de l'éducation. Il relève des dispositions réglementaires des articles D.713-1 à D.713-4 du code de l'Education relatif aux instituts universitaire de technologie.

- Le présent règlement intérieur a pour but : de définir les règles de comportement qui doivent être respectées au sein de l'Institut Universitaire de Technologie (IUT) ;
- de préciser le mode de fonctionnement des différentes instances de l'IUT ;
- d'assurer la bonne information au sein de l'IUT.

Il respecte les principes énoncés en préambule du règlement intérieur de l'Université, aux termes duquel :

« Conformément à l'article L. 141-6 du Code de l'Education « le service public de l'enseignement supérieur est laïque et indépendant de toute emprise politique, économique, religieuse et idéologique ; il tend à l'objectivité du savoir ; il respecte la diversité des opinions. » Dans l'exercice de ses missions, l'université promeut le développement durable et les valeurs d'humanisme, et réaffirme le principe de laïcité, qui figure au nombre des droits et libertés que la Constitution garantit.

L'Université condamne toutes les discriminations et toute forme de harcèlement. Elle promeut l'égal accès des femmes et des hommes aux fonctions électives et responsabilités professionnelles et sociales.

L'Université s'est par ailleurs engagée résolument dans la voie du développement durable. Elle est signataire de la « Charte pour une alliance des Universités françaises en faveur du développement durable ». En conséquence conformément à ses statuts, elle entend promouvoir les comportements respectueux de l'environnement et mettre en œuvre les moyens d'une politique audacieuse dans les domaines du développement durable.
L'université s'engage à agir conformément aux bonnes pratiques définies dans la charte du développement durable. »

Article 2. Destinataires du règlement intérieur

Le règlement intérieur s'applique à tous les personnels permanents et occasionnels de l'IUT, quels que soient leur statut et leur employeur, ainsi qu'à tous les apprenants (étudiants en formation initiale, alternants et stagiaires de la formation continue). Il s'impose aussi à toute personne physique ou morale au sein de l'IUT.

Article 3. Comportement général et usage des locaux

Par délégation du Président de l'Université, le directeur de l'IUT est responsable du maintien de l'ordre et veille au respect du présent règlement intérieur ainsi que de la sécurité, de l'hygiène et de la salubrité dans l'enceinte et dans les locaux de l'IUT.

Toute personne présente à quelque titre que ce soit dans les locaux de l'IUT doit avoir un comportement correct (notamment dans ses actes, attitudes, propos ou tenue). La même règle s'applique, à l'extérieur, aux apprenants et aux membres du personnel lorsqu'ils représentent l'IUT.

Le bizutage, défini comme « le fait pour une personne d'amener autrui, contre son gré ou non, à subir ou à commettre des actes humiliants ou dégradants ou à consommer de l'alcool de manière excessive, lors de manifestations ou de réunions liées aux milieux scolaire, sportif et socio-éducatif » constitue un délit, prévu et réprimé par le code pénal (art. 225-1-16 et suivants et art. L. 811-4 du code de l'éducation). Il est à ce titre interdit dans l'enceinte comme en-dehors de l'IUT.
Les auteurs de faits de bizutage, comme les personnels de l'IUT s'il est avéré qu'ils ont, par leur comportement, organisé, encouragé, facilité le bizutage ou s'ils se sont abstenus de toute intervention

pour les empêcher, sont passibles de poursuites disciplinaires, sans préjudice d'éventuelles poursuites pénales, y compris lorsque les faits ont été commis à l'extérieur de l'établissement.

Toutes les manifestations organisées au sein de l'établissement doivent faire l'objet d'une demande préalable auprès du Directeur de l'IUT.

La consommation d'alcool est interdite à l'intérieur des bâtiments et des enceintes de l'IUT.
Des dérogations pourront être accordées notamment dans le cas de manifestations exceptionnelles par le directeur de l'IUT, sur délégation du président.
La vente d'alcool est interdite dans tous les cas et il est obligatoire de proposer des boissons non-alcooliques. La délivrance de boissons alcooliques aux mineurs est interdite.
La consommation de stupéfiants est prohibée.
Il est interdit de fumer et d'utiliser la cigarette électronique dans les locaux de l'IUT.
Afin d'éviter la propagation des fumées à l'intérieur des locaux, il est également interdit de fumer ou d'utiliser la cigarette électronique sous les fenêtres, sur les balcons, perrons, escaliers et paliers extérieurs, dans les patios et les cours intérieures, ainsi que sous les porches, préaux et auvents des bâtiments.
Les règles d'utilisation des ressources informatiques et les responsabilités des utilisateurs sont fixées par la charte régissant l'usage des technologies de l'information et de la communication par les utilisateurs, la charte régissant l'usage du système d'information par les organisations syndicales et le protocole de gestion des journaux informatiques à l'Université Toulouse 1 Capitole, qui sont annexés au présent règlement intérieur.
Sans préjudice d'éventuelles poursuites disciplinaires, l'accès aux salles et ressources informatiques peut être temporairement interdit aux contrevenants aux dispositions de la charte régissant l'usage des technologies de l'information et de la communication, sur décision du directeur de l'IUT qui entend préalablement les intéressés..

Article 4. Protection des données à caractère personnel

La manipulation de données à caractère personnel est encadrée par le règlement général sur la protection des données (RGPD) et la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée. Toute opération portant sur des données à caractère personnel, liée à la gestion de l'établissement doit respecter cette réglementation.

- *Article 4-1. Responsable du traitement*

Le responsable du traitement des données à caractère personnel est le Directeur de l'IUT de Rodez, composante de l'Université Toulouse 1 Capitole (UT1).

- *Article 4-2. Traitements des données et finalités*

Conformément à l'article 6 du règlement européen sur la protection des données, les traitements de données à caractère personnel sont effectués par l'IUT de Rodez pour les motifs suivants :

- L'**exécution**, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à sa demande,
- Le **respect d'une obligation légale** incombant à l'établissement,
- L'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement,
- La réalisation d'un **intérêt légitime** poursuivi par l'organisme ou par le destinataire des données, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Concernant les deux derniers motifs, les destinataires du présent règlement intérieur précisés à l'article 2 disposent d'un droit d'opposition au traitement de leurs données pour des raisons tenant à leur situation particulière.
Les informations recueillies sur les destinataires du présent règlement intérieur précisés à l'article 2 font l'objet de traitements papiers ou informatiques ayant pour finalités la gestion administrative des personnes, l'organisation du travail et des études, la mise à disposition d'outils informatiques, la réalisation d'études statistiques et de prospective ou encore, pour les membres du personnel, la gestion des carrières et la formation.
La **durée de conservation** des données est définie comme suit : pour les membres du personnel : 80 ans à compter de la date de naissance du personnel,
Les **destinataires des données** à caractère personnel sont les personnes et services habilités chargés de la gestion du personnel et des usagers, les supérieurs hiérarchiques des agents, les instances

représentatives du personnel, les services chargés d'études à des fins statistiques et de prospective dans le respect de la limitation du traitement de celles-ci, conformément à l'article 5 du RGPD.

- *Article 4-3. Exercice des droits*

Dans le cadre des traitements de données à caractère personnel effectués par l'IUT de Rodez, les destinataires du présent règlement intérieur précisés à l'article 2 disposent d'un droit d'accès, de rectification et de limitation des traitements des données à caractère personnel les concernant.
Ils disposent également d'un droit d'opposition, tel que prévu à l'article 21 du RGPD pouvant être exercé en contactant le (la) Référent(e) RGPD de l'IUT de Rodez par courrier à : IUT de Rodez, à l'attention du référent RGPD, 50 avenue de Bordeaux 12000 Rodez, ou par courriel à l'adresse : **rgpd@iut-rodez.fr** ou le (la) Délégué(e) à la Protection des Données par courrier à : Direction Générale des Service, à l'attention du Délégué à la Protection des Données, Université Toulouse 1 Capitole, 2 Rue du Doyen Gabriel Marty 31042 Toulouse Cedex 9, ou par courriel à l'adresse : **dpo@ut-capitole.fr**
Pour garantir l'exercice effectif de ces droits, ils doivent justifier de leur identité par tout moyen.
Les membres du personnel et les usagers sont informés par le présent règlement que s'ils estiment que leurs droits en matière de données personnelles ne sont pas respectés, ils sont en droit de saisir le Service des plaintes de la Commission Nationale de l'Informatique et Libertés (CNIL) en lui adressant un courrier simple.

TITRE II - Dispositions relatives aux apprenants

Article 5. Information des apprenants

Les apprenants sont tenus informés des dispositions prises grâce à la participation de leurs représentants :

- au Conseil de l'IUT ;
- au Conseil de leur département ;
- aux Conseils de l'Université et notamment à la CFVU ;
- au CROUS.

Ils sont également informés des dispositions les concernant dans les statuts de l'Institut, consultables à la direction et sur le site internet de l'IUT de Rodez, ainsi que dans le présent règlement intérieur.

Article 6. Présence

- *Article 6-1. Obligation d'assiduité*

L'assiduité à toutes les activités pédagogiques organisées dans le cadre de la formation est obligatoire.
Le présent règlement intérieur adopté par le conseil de l'IUT définit les modalités d'application de cette obligation.

- *Article 6-2. Déclaration des absences*

Les absences prévisibles doivent être déclarées par écrit, téléphone ou courrier électronique, dès connaissance de celles-ci, auprès du secrétariat du Département.
Les absences imprévues doivent être déclarées par écrit, téléphone ou courrier électronique, dès la première journée d'absence, auprès du secrétariat de chaque Département dont l'apprenant a manqué une séance d'enseignement.

- *Article 6-3. Justification des absences*

Toute absence est a priori considérée comme injustifiée.
Toute absence doit être justifiée dans les 48 heures qui suivent la déclaration d'absence, par le dépôt d'un justificatif (certificat, attestation, convocation) auprès du secrétariat du Département.
Sont reconnus comme recevables les motifs d'absences suivants :

- L'absence en cas de maladie, sur présentation d'un certificat médical qui doit préciser le nombre de journées d'absences (arrêt de travail pour les alternants et stagiaires de la formation continue) ;
- Décès d'un proche avec certificat de décès ;
- Epreuve du permis de conduire (sur présentation de la convocation) ;
- Obligations administratives (sur convocation ou justificatif) ;

- Entretien de stage ou d'embauche à titre exceptionnel avec accord préalable du Chef de Département ;
- Convocation à un examen ou à un concours.

La justification est laissée, en dehors de ces cas, à l'appréciation du Chef de Département qui convoquera et entendra l'apprenant.

- *Article 6-4. Sanctions en cas d'absences injustifiées*

Le contrôle de l'assiduité est placé sous la responsabilité de chaque enseignant. Chaque Chef de Département tient à disposition des commissions et des jurys, un relevé précis des absences des apprenants.
Les moyennes générales des unités d'enseignements ne peuvent être calculées que si l'obligation d'assiduité est satisfaite.
Les absences sont comptabilisées en séance d'enseignement dans chaque activité pédagogique.
Pour chaque activité pédagogique, une pénalité sur la notation peut être appliquée par l'enseignant en cas d'absence injustifiée.
Dès la première absence injustifiée dans un semestre, l'apprenant peut faire l'objet d'une convocation par le Chef de Département. A la cinquième, ce dernier reçoit par écrit une notification du cumul de ses absences. A la septième absence, l'apprenant peut être considéré comme défaillant par les commissions et les jurys : ses moyennes ne sont pas calculées et il ne peut prétendre à la validation des unités d'enseignements.
Les sanctions prévues au présent article ne sont pas exclusives de celles prévues à l'article 8.

Article 7. Obligation de comportement de l'apprenant

- *Article 7-1. Renvoi ponctuel d'un apprenant*

Sans préjudice d'éventuelles poursuites devant la section disciplinaire de l'Université, le renvoi ponctuel d'un apprenant durant une activité pédagogique peut être décidé par l'enseignant en charge d'un enseignement notamment dans les cas suivants :

- retards importants et/ou systématiques de l'apprenant aux enseignements sans justification valable, celle-ci étant laissée à l'appréciation de l'enseignant ;
- comportement indiscipliné, récurrent, perturbant manifestement le cours, malgré des rappels à l'ordre de l'enseignant ;
- propos ou gestes grossiers ou injurieux ;

Toute exclusion de cours conduit à noter l'apprenant absent. Cette absence est considérée comme une absence injustifiée.

- *Article 7-2. Notification d'un renvoi ponctuel*

La mesure temporaire de renvoi doit être notifiée et motivée par l'enseignant au Chef de Département. Elle est effective pour la durée de l'enseignement où l'incident s'est produit. Elle est enregistrée comme une absence injustifiée.

Article 8. Fraude et sanctions disciplinaires

- *Article 8-1. Conseil de discipline*

Tout usager de l'IUT lorsqu'il est auteur ou complice, notamment :
1° D'une fraude ou d'une tentative de fraude commise notamment à l'occasion d'une inscription, d'une épreuve de contrôle continu, d'un examen ou d'un concours ;
2° De tout fait de nature à porter atteinte à l'ordre, au bon fonctionnement ou à la réputation de l'université ou de l'institut,
est passible de sanctions décidées par le conseil académique constitué en section disciplinaire de l'Université Toulouse 1 Capitole (UT1).
Le responsable sera traduit devant le conseil académique constitué en section disciplinaire de UT1. Conformément à l'article R811-36 du Code de l'éducation, ces sanctions peuvent être :

- l'avertissement ;
- le blâme ;
- la mesure de responsabilité définie au titre II de l'article R811-36 du Code de l'éducation ;
- l'exclusion de l'établissement pour une durée maximum de 5 ans. Cette sanction peut être prononcée avec sursis si l'exclusion n'excède pas 2 ans ;

- l'exclusion définitive de l'établissement ;
- l'exclusion de tout établissement public d'enseignement supérieur pour une durée maximum de 5 ans ;
- l'exclusion définitive de tout établissement public d'enseignement supérieur.

Tous documents et matériels (calculatrices, portables, agendas et organiseurs électroniques, montres connectées etc..) sont interdits lors des épreuves, sauf si l'enseignant responsable de l'épreuve le spécifie.

- *Article 8-2. Plagiat*

Les apprenants sont encouragés à citer les travaux ou écrits d'autrui, mais en indiquant précisément leurs sources suivant les normes propres à chaque discipline. Il appartiendra aux enseignants de leur indiquer ces normes. Citer ou paraphraser le travail d'autrui sans nommer ses sources ou sans user de guillemets dans l'intention de le faire passer pour sien constitue un plagiat. Le délit de contrefaçon ainsi constitué peut donner lieu, indépendamment de la mise en œuvre de poursuites pénales, à une sanction disciplinaire.

Article 9. Modalités de contrôle des connaissances

Le Conseil de l'IUT statue sur les modalités de contrôle des connaissances. Elles sont rendues publiques au plus tard à la fin du premier mois de l'année d'enseignement, après leur adoption par la Commission de la Formation et de la Vie Universitaire.

Article 10. Conditions de passage des épreuves

L'absence d'un apprenant à un contrôle entraîne automatiquement la note de 0.
Toutefois, le responsable de la formation examine obligatoirement la situation de l'apprenant absent et peut l'autoriser à subir un contrôle de remplacement qui pourra prendre une autre forme que le contrôle initial. Dans ce cas, la nouvelle note sera substituée au 0.
Cette possibilité n'est offerte qu'aux apprenants fournissant :

- un certificat médical attestant une incapacité à passer une épreuve ou un examen,
- une pièce justificative permettant d'établir un autre motif d'absence impérieux et légitime : dans ce dernier cas, la décision est laissée à l'appréciation du Chef de Département.

Article 11. Associations

Toute domiciliation d'une association à l'IUT doit être au préalable soumise à autorisation du Directeur. C'est à cette condition que l'association pourra bénéficier des services d'accompagnement proposés par l'IUT.
Seules les associations exerçant des activités compatibles et en relation avec la mission de service public de l'IUT peuvent se voir accorder la domiciliation à l'IUT.
La demande d'autorisation, par lettre manuscrite accompagnée du projet de statuts, doit être déposée auprès du secrétariat de la Direction (direction@iut-rodez.fr).
Le Directeur de l'IUT enverra une réponse écrite d'accord ou de refus motivé.

Article 12. Clause de révision du règlement intérieur

Le règlement intérieur est adopté, après consultation du CHSCT et du CT, par le Conseil de l'IUT de Rodez, par la CFVU et le CA de l'Université à la majorité des suffrages exprimés ; il peut être modifié dans les mêmes conditions.

ANNEXES :

- Charte régissant l'usage des technologies de l'information et de la communication par les utilisateurs de l'Université Toulouse 1 Capitole ;

- Charte régissant l'usage du système d'information par les organisations syndicales de l'Université Toulouse 1 Capitole ;

- Protocole de gestion des journaux informatiques à l'Université Toulouse 1 Capitole.

CONSEIL D'ADMINISTRATION - Séance du 17/12/2019
DELIBERATION n° CA - 2019 - 13

Charte régissant l'usage des technologies de l'information et de la communication par les utilisateurs de l'Université Toulouse 1 Capitole

Préambule

Par "système d'information" s'entend l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'Université Toulouse 1 Capitole, nommée ci-après l'UT1.

L'informatique nomade tels que les assistants personnels, les ordinateurs portables, les téléphones portables, etc. est également un des éléments constitutifs du système d'information.

Par « utilisateur », s'entend toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle ou en tant qu'usager, aux ressources du système d'information, quel que soit son statut.

Ainsi sont notamment désignés :

- Tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'établissement ;
- Tout usager des services de l'UT1 ;
- Tout personnel hébergé par l'université que ce soit dans le cadre de coopération de recherche, d'enseignement, de collaboration administrative ou de manifestations ;
- Tout prestataire[1] ayant contracté avec l'UT1 ;
- Tout visiteur extérieur bénéficiant d'un usage de ces ressources.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente charte définit les règles d'usages et de sécurité que l'UT1 et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

La charte est accompagnée d'un guide juridique qui rappelle les dispositions législatives en vigueur pour son application. Elle peut être complétée par des guides d'utilisation définissant les principales règles pratiques d'usage.

Engagements de l'UT1

L'UT1 porte à la connaissance de l'utilisateur la présente charte.

L'UT1 met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'UT1 facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'UT1 est tenue de respecter la vie privée de chacun.

Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie[2].

1 Le contrat devra prévoir expressément l'obligation de respect de la charte.
2 Notamment le secret médical dans le domaine de la santé.

Les utilisateurs ont une responsabilité particulière dans l'utilisation qu'ils font des ressources mises à leur disposition par l'UT1.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

Article I. Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'UT1 ainsi qu'à l'ensemble des utilisateurs.

Les usages relevant de l'activité des organisations syndicales sont régis par une charte spécifique qui complète le présent document.

Article II Conditions d'utilisation des systèmes d'information

Section II.1 Utilisation professionnelle / privée

Les communications électroniques (messagerie, internet ...) sont des outils de travail ouverts à des usages professionnels administratifs et pédagogiques et peuvent constituer le support d'une communication privée.

L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence, son volume que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

Le caractère privé des données est subordonné à l'utilisation du mot clé PRIVE (en majuscule et sans accent) qui devra être utilisé notamment pour le nom des répertoires et dans le sujet des courriers électroniques.

L'utilisateur est seul responsable de la protection et de la conservation de ses données à caractère privé.

Section II.2 Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition.

En cas d'absence non planifiée et pour des raisons exceptionnelles, si un utilisateur se trouve dans l'obligation de communiquer ses codes d'accès aux services chargés des systèmes d'information, il doit procéder, dès que possible, au changement de ces derniers ou en demander la modification à l'administrateur. L'administrateur est soumis à la présente charte informatique. Il doit, d'une manière générale, respecter les règles d'éthique professionnelle et de déontologie, l'obligation de réserve, le devoir de discrétion ainsi que l'obligation de confidentialité des

informations auxquelles il a accès. Il doit mettre en œuvre des mesures visant à assurer leur non divulgation.

En cas d'indisponibilité de l'utilisateur pour communiquer ses codes d'accès au système d'information, son (sa) supérieur(e) hiérarchique peut demander au service informatique de proximité d'accéder à tous les documents et informations professionnels à l'exclusion des données à caractère privé telles que définies à la section II.1.

Lors de son départ définitif du service ou de l'établissement, il incombe à l'utilisateur de s'assurer de la transmission des données professionnelles dans le service. Il lui appartient de détruire ses données à caractère privé. L'administration n'est pas responsable des données à caractère privé qui pourraient rester dans les systèmes d'information après le départ de l'utilisateur.

Article III. Principes de sécurité

Section III.1 Règles de sécurité applicables

L'UT1 met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée ou des accès aux services numériques qui lui sont autorisés. La sécurité des systèmes d'information mis à sa disposition lui impose :

- De respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;
- De garder strictement confidentiels son (ou ses) codes d'accès[3] et ne pas le(s) dévoiler à un tiers (sauf cas prévus en section 2.2) ;
- De respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaitre.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

De la part de l'UT1 :

- Veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie (Cf. section 2.2) ;
- Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

De la part de l'utilisateur :

- S'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;
- Ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou

3 Identifiants, mots de passe, dispositifs d'accès logique ou physique (carte à puce, clés de sécurité ...)

autorisés par l'UT1, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou l'établissement ;

- Ne pas installer, télécharger ou utiliser sur le matériel de l'UT1, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de sa hiérarchie ou du service habilité à donner cette autorisation ;
- Se conformer aux dispositifs mis en place par l'UT1 pour lutter contre les codes malveillants et les attaques par programmes informatiques.

Devoirs de signalement et d'information

L'UT1 doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information.

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. Il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation.

Section III.2 Mesures de contrôle de la sécurité

L'utilisateur est informé :

- Que pour effectuer la maintenance corrective, curative ou évolutive, l'UT1 se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- Qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- Que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée.

L'UT1 informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle des systèmes d'information ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que :

- Ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles (Cf. Section II.1), elles relèvent de la vie privée de l'utilisateur ;
- Elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, elles ne tombent pas dans le champ de l'article 40[4] alinéa 2 du code de procédure pénale.

Article IV. Communications électroniques

Section IV.1 Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du

4 Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.

travail, de mutualisation et d'échange de l'information au sein de l'UT1.

Adresses électroniques

L'UT1 s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

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

L'adresse électronique nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

Une adresse électronique[5], fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'UT1.

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'UT1 : ces adresses ne peuvent être utilisées sans autorisation explicite.

Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte la mention particulière PRIVE dans le sujet du message.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place: dans ce cas, les termes en sont précisés dans un guide technique d'utilisation de la messagerie qui est porté à la connaissance des utilisateurs.

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 de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui.

L'utilisation de la messagerie professionnelle par les organisations syndicales depuis les systèmes d'informations de l'UT1, est régie par la charte relative aux usages syndicaux.

Émission et réception des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

L'UT1 procède à des campagnes de filoutage (« phishing ») pour sensibiliser et prévenir les utilisateurs des risques encourus.

Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1125 et suivants du code civil.

L'utilisateur doit en conséquence, être vigilant sur la nature des messages électroniques

5 L'adresse est de la forme prenom.nom@ut-capitole.fr, parfois prenom+numero.nom@ut-capitole.fr

qu'il échange au même titre que pour les courriers traditionnels.

Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

A ce titre, il doit notamment se conformer aux règles définies dans la présente charte et, le cas échéant, dans le ou les guides d'utilisation établi par le service ou l'établissement.

Section IV.2 Internet

L'UT1 est signataire de la charte RENATER (Réseau National de télécommunications pour la Technologie l'Enseignement et la recherche), accessible sur https://www.renater.fr/IMG/pdf/charte_fr.pdf. Dans ce cadre, elle se doit de faire respecter les règles déontologiques qui y sont décrites. Par ailleurs, il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'UT1.

L'UT1 met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques) : il peut constituer le support d'une communication privée telle que définie en section 2.02 dans le respect de la législation en vigueur.

En complément des dispositions légales en vigueur et au regard de la mission éducative de l'UT1, la consultation volontaire et répétée de sites à contenus de caractère pornographique depuis les locaux de l'UT1, est interdite.

Publications sur les sites internet et intranet de l'UT1

Toute publication de pages d'information sur les sites internet ou intranet de l'UT1[6] doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé (pages privées ...) sur les ressources du système d'information de l'UT1 n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou l'établissement.

Sécurité

L'UT1 travaille à améliorer sa conformité à la politique de sécurité des systèmes d'information de l'Etat[7]. Cela impose un certain nombre de règles et procédures qui s'appliquent aussi bien à l'établissement qu'aux utilisateurs.

L'UT1 se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

Les utilisateurs doivent privilégier dans leurs activités professionnelles les outils numériques et applications mis à disposition par l'établissement.

---

6 A partir des ressources informatiques mises à la disposition de l'utilisateur

7 https://www.ssi.gouv.fr/entreprise/reglementation/protection-des-systemes-dinformations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'UT1. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'établissement.

L'UT1 procède régulièrement à des tests de sécurité. Ces tests de sécurité peuvent déclencher des mesures de protections pouvant bloquer temporairement l'accès aux systèmes d'informations aux utilisateurs.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de campagnes de sensibilisation.

Section IV.3 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article VI.

L'UT1 se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'UT1, codes malveillants, programmes espions ...).

Article V. Traçabilité

L'UT1 est dans l'obligation légale de mettre en place un système de journalisation[8] des accès Internet, de la messagerie et des données échangées.

L'UT1 se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information.

Préalablement à cette mise en place, l'UT1 procèdera, auprès de la Commission nationale de l'informatique et des libertés, à une déclaration, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 du 6 janvier 1978 modifiée.

Article VI. Respect de la propriété intellectuelle

L'UT1 rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

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.

Article VII. Respect de la loi informatique et libertés

Section VII.1 Obligations des utilisateurs

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6

8 Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur, voir à cet effet le Protocole de gestion des journaux informatiques à l'Université Toulouse 1 Capitole.

janvier 1978 dite « Informatique et Libertés » modifiée et au règlement européen sur la protection des données personnelles (RGPD) (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés » et au RGPD.

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement le délégué à la protection des données qui prendra les mesures nécessaires au respect des dispositions légales.

Section VII.2 Droits des agents et des usagers

Conformément aux dispositions de la loi « Informatique et Libertés » et du RGPD précités, chaque utilisateur dispose d'un droit d'accès, de suppression, de portabilité, de limitation et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'Information. L'utilisateur peut également définir des directives relatives au sort de ses données à caractère personnel après sa mort.

Ces droits s'exercent en contactant le Délégué à la Protection des Données par courrier (Direction Générale des Services, à l'attention du Délégué à la Protection des Données, Université Toulouse 1 Capitole, 2 Rue du Doyen Gabriel Marty 31042 Toulouse Cedex 9) ou par courriel (dpo@ut-capitole.fr).

Les utilisateurs sont informés par la présente charte que s'ils estiment que leurs droits en matière de données personnelles ne sont pas respectés, ils sont en droit de saisir le Service des plaintes de la Commission Nationale de l'Informatique et Libertés (CNIL) en lui adressant un courrier simple.

Article VIII. Limitations des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation établi par le service ou l'établissement, la « personne juridiquement responsable » pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.

Par « personne juridiquement responsable », on entend le Président de l'Université Toulouse 1 Capitole.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra- professionnelles, est passible de sanctions.

Article IX. Dispositions finales

La présente charte est annexée au règlement intérieur de l'Université Toulouse 1 Capitole. Elle a été adoptée, après consultation du CHSCT et du CT, par le Conseil d'Administration de l'établissement lors de sa séance du 17 décembre 2019.

Charte régissant l'usage du système d'information par les organisations syndicales de l'Université Toulouse 1 Capitole

Sommaire

Préambule

La présente charte définit les conditions d'utilisation du système d'information par les organisations syndicales dans le cadre de l'exercice de leur activité dans la fonction publique.

Par « organisation » ou « organisation syndicale », il faut entendre toute organisation syndicale représentative au sein de l'université Toulouse 1 Capitole, conformément aux critères légaux et jurisprudentiels en vigueur. Ces critères s'appliquent au ressort territorial concerné.

Le terme d' «institution» représente l'université Toulouse 1 Capitole.

La présente charte formalise les conditions de mise à disposition par l'institution des outils de communication électronique tels que la messagerie électronique interne de l'administration ou les intranets institutionnels dans des conditions permettant de faciliter et de préserver tout à la fois :

- *le droit à l'expression syndicale,*
- *l'égalité de traitement des différents partenaires sociaux,*
- *l'intégrité de l'outil de travail, propriété de l'institution*

Champ d'application

La présente charte précise les modalités d'utilisation des systèmes d'information par les organisations syndicales citées dans le préambule, sans que celles-ci puissent se substituer aux moyens d'expression existants et régis par le décret 82-447 du 28 mai 1982 relatif à l'exercice du droit syndical dans la fonction publique.

Messagerie électronique

Attribution d'adresses électroniques syndicales

L'institution s'engage à attribuer à l'organisation syndicale une adresse électronique lui permettant d'émettre et de recevoir des messages.

La dénomination de cette adresse syndicale devra faire apparaître explicitement le nom[1] de l'organisation.

L'adresse électronique de l'organisation syndicale ne se substitue pas à celle de l'agent représentant de l'organisation ; ainsi celui-ci devra-t-il utiliser l'adresse fonctionnelle pour toute communication d'expression syndicale.

L'accès à ces adresses est autorisé depuis tout poste de travail, le cas échéant, depuis un poste mis à disposition par l'institution (inspections académiques, rectorats ou administration centrale).

Nature des messages électroniques

Les adresses électroniques syndicales ont vocation à être utilisées prioritairement pour la vie interne des syndicats, notamment pour la correspondance avec les adhérents, sans autre limitation que celles définies dans la charte régissant l'usage du système d'information par les personnels.

L'adresse électronique de l'organisation syndicale peut servir aux échanges avec tout personnel de l'institution de façon individualisée (à l'initiative de l'agent) ou par le biais de listes de diffusion préétablies (Cf. section 2.03).

Pour la diffusion d'informations syndicales à caractère général, l'organisation syndicale utilise la publication sur l'espace intranet qui lui est réservé et non l'envoi de masse sur les adresses de messagerie des personnels : les conditions d'utilisation d'intranet sont précisées à l'article III.

Listes de diffusion

Les organisations syndicales ont la possibilité d'établir, sous leur seule responsabilité et avec l'accord préalable des agents, des listes privées de destinataires. Ces listes de diffusion permettent aux organisations syndicales de diffuser une information syndicale à caractère général.

L'inscription sur la liste privée résulte d'un acte volontaire de l'agent. La présence d'un agent sur plusieurs listes est possible.

L'inscription peut se faire en ligne à partir du site syndical ou de l'espace d'expression Intranet dédié à chaque organisation syndicale. Tous les agents figurant sur ces listes peuvent demander à tout moment à en être radiés. Les organisations syndicales sont tenues de faire droit à ces demandes.

L'institution s'engage à faire connaître aux agents l'existence de ces listes en envoyant un message, au moins une fois par an, à l'ensemble des agents de son ressort les informant de la possibilité pour eux de s'abonner à une liste de diffusion syndicale à partir de l'espace Intranet dédié.

[1] Pour exemple <nom de l'organisation syndicale>@< nom de domaine de l'institution> ou <nom de l'organisation syndicale>.<complément contextuel>@< nom de domaine de l'institution>

La dénomination des listes doit faire apparaître explicitement le nom de l'organisation syndicale[2]. La déclaration à la CNIL de l'existence des listes de diffusion relève de la responsabilité de chaque organisation syndicale.

Les listes de diffusion sont gérées par les organisations syndicales qui reçoivent les inscriptions et les radiations.

Confidentialité des échanges

L'institution s'engage à prendre les mesures appropriées en vue d'assurer la confidentialité :

- des messages électroniques en provenance ou à destination d'adresses électroniques fonctionnelles syndicales (contenu, auteurs et destinataires),
- la liste des adresses contenues dans la liste de diffusion élaborée par l'organisation syndicale.

Tout auteur d'actes d'interception de correspondances s'expose à des sanctions pénales et/ou disciplinaires.

L'institution dégage toute responsabilité sur des faits qui seraient commis par un tiers.

Accès des organisations syndicales à l'Intranet

Droits d'usage

L'institution s'engage à mettre à disposition de l'organisation syndicale un espace de publication sur son intranet institutionnel[3]. Un lien en page d'accueil permettra de renvoyer vers les pages d'expression syndicale.

L'ouverture de cet espace dédié s'effectue sur demande explicite de l'organisation syndicale. Il permet la mise à disposition de tout personnel des informations d'expression syndicale sous la responsabilité de l'organisation syndicale.

L'accès aux applications métiers (applications de gestion des ressources humaines, …) n'est pas autorisé aux organisations syndicales. Un accès partiel peut faire l'objet d'un accord formel à l'initiative de l'institution.

Gestion de l'espace dédié et de ses contenus

L'organisation syndicale s'engage à limiter sur son espace dédié la publication aux seules informations d'expression syndicale avec la possibilité de renvois vers d'autres sites syndicaux sur l'intranet ou l'internet.

Formation

Une formation peut être mise en place pour permettre aux représentants de l'organisation syndicale qui le souhaitent d'acquérir les compétences nécessaires à la mise en ligne des pages sur l'espace intranet réservé.

---

2 Pour exemple, Liste. <nom de l'organisation syndicale>@< nom de domaine de l'institution> ou liste. <nom de l'organisation syndicale>.<complément contextuel>@< nom de domaine de l'institution> >

3 Serveur intranet ou ENT

Statut et valeur juridique des contenus

La mise en ligne des informations sur l'espace dédié s'effectue sous la responsabilité éditoriale de l'organisation syndicale : une mention sur la page d'accueil de l'espace dédié à l'organisation syndicale le précisera.

Le contenu de ces intranets ne saurait engager la responsabilité civile ou pénale de l'institution.

L'organisation syndicale doit :

- respecter strictement les lois et règlements relatifs au droit d'expression syndicale, au droit de la presse, à l'abus de droit et au droit d'auteur ;

- procéder à toutes les déclarations lui incombant auprès de la commission nationale informatique et liberté, en particulier lors de la constitution des listes de diffusion.

La nature et le contenu des pages d'information pourront faire l'objet d'éventuelles contestations devant les juridictions compétentes.

Mesures conservatoires

En cas d'inobservation des termes de la présente charte, des lois et des règlements en vigueur, l'institution se réserve le droit de suspendre, à titre conservatoire, tout accès aux services tels que définis aux sections 2.01 et 3.01.

Entrée en vigueur de la charte

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'information de l'institution par les organisations syndicales.

Protocole de gestion des journaux informatiques à l'Université Toulouse 1 Capitole

Définitions

- on entend par « établissement » « l'Université Toulouse 1 Capitole » ;
- on entend par « utilisateur » les personnels, étudiants, stagiaires, personnes invitées et en règle générale toute personne utilisant les moyens du système d'information ;
- on entend par « entités » les composantes, services ou laboratoires...

Contexte

Le fonctionnement de l'établissement passe par l'utilisation de systèmes d'information et de moyens de communications qui s'appuient sur des réseaux télématiques connectés à l'échelle mondiale. Ces réseaux, qui apportent une souplesse inégalée, ont également une grande vulnérabilité intrinsèque, et leur utilisation engage la responsabilité personnelle des utilisateurs, ainsi que dans certaines situations celle de l'établissement qui met ces moyens à leur disposition en tant qu'outils de travail.

L'utilisation des nouvelles technologies de communication pose le problème de la protection d'une part de l'information sensible[1] gérée par les utilisateurs et d'autre part des systèmes d'information sous la responsabilité de l'établissement. Les mesures mises en œuvre doivent permettre à l'établissement de remplir ses missions tout en satisfaisant aux exigences qui sont imposées par ses engagements vis-à-vis de ses partenaires, des réglementations sur la protection des données sensibles et la protection du patrimoine scientifique, de la loi sur la protection des données à caractère personnel (respect des droits de l'individu) et la sécurité des systèmes d'information.

Une déontologie et un contrôle de l'utilisation sont donc nécessaires, de même qu'une information et une sensibilisation des utilisateurs. L'établissement a mis en place des dispositions et moyens pour assurer la sécurité et le contrôle de l'utilisation des moyens télématiques, et d'autre part a fixé les conditions d'utilisation de ces moyens, afin de garantir les droits individuels de chaque utilisateur.

Principes de base

Une maitrise de la fiabilité et de la sécurité du fonctionnement des systèmes d'information et une garantie de la légalité des transactions opérées nécessitent un contrôle s'appuyant nécessairement sur l'enregistrement systématique et temporaire d'un certain nombre d'informations caractérisant chaque transaction, appelées journaux informatiques (ou logues).

Finalités des traitements

Les traitements de ces journaux informatiques ont pour finalités :

- de contrôler le volume d'utilisation de la ressource, détecter des anomalies afin de mettre en place une qualité de service et faire évoluer les équipements en fonction des besoins (métrologie) ;
- de vérifier que les règles en matière de sécurité des systèmes d'information (SSI) sont correctement appliquées ;

1 Informations sensibles au sens où la confidentialité (contrat, données de recherche, information nominatives, ..), l'intégrité (informations de gestion,...) et la disponibilité nécessitent une protection particulière.

- de détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ;
- de détecter toute violation de la loi ou tout abus d'utilisation des moyens informatiques pouvant engager la responsabilité de l'établissement ;
- de détecter les utilisations des moyens informatiques contraires aux chartes ou au règlement intérieur de l'établissement.
- d'être à même de fournir les éléments de preuves nécessaires pour mener les enquêtes en cas d'incident et de répondre à toute réquisition de l'autorité judiciaire présentée dans les formes légales.

Les finalités précitées imposent d'aller au-delà d'un enregistrement et d'une exploitation de données statistiques. Ils impliquent nécessairement l'enregistrement, la conservation temporaire et l'éventuelle exploitation de données à caractère personnel, dans la mesure où des éléments contenus dans les traces permettraient de remonter à l'utilisateur.

Ces journaux et leur traitement doivent respecter les droits de chacun et notamment être conformes à la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 dite loi "Informatique et libertés". Ils doivent avoir satisfait au principe d'information préalable et de transparence ainsi qu'au régime déclaratif en vigueur auprès de la CNIL[2].

Durée de conservation

La durée de conservation des journaux informatiques est de 1 an maximum. L'établissement s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme. Deux conteneurs de données sont donc définis, le premier reçoit les fichiers de logues vieux de moins de trois mois et les fichiers anonymisés quand ils existent. Le second reçoit les journaux contenant des données à caractère nominatif de plus de trois mois

Qualités des données collectées

Les informations journalisées doivent être factuelles et contextuelles, c'est à dire qu'elles doivent permettre de connaitre l'environnement de la collecte, le système hôte, les logiciels mis en œuvre etc.

L'heure relevée est une information importante parce qu'elle est souvent le premier élément utilisé pour rapprocher des journaux de différents serveurs. Il est donc indispensable que les machines produisant des logues soient synchronisées sur un serveur de temps,

D'éventuelles interruptions de la journalisation doivent être repérables par les destinataires de ces données.

Sécurité et intégrité des données

La politique de sécurité du système d'information (PSSI) fixe les règles de sécurité appliquées à ces fichiers. Ces règles assurent l'intégrité des données en les protégeant en particulier contre un effacement ou des modifications malveillantes. Au besoin, une base d'empreintes numériques ou des jetons d'horodatage permettent de surveiller l'intégrité des fichiers de journaux.

---

2 Voir la fiche pratique relative au contrôle de l'utilisation des moyens informatiques dans le Guide pratique Informatique et Libertés" pour l'enseignement supérieur et la recherche (ce guide est disponible sur le site de la CNIL et celui de l'AMUE)

Les règles de sécurité limitent l'accès aux fichiers de logues de moins de trois mois aux seuls administrateurs destinataires de ces données tel qu'ils sont définis au paragraphe 4.2.1 avec authentification préalable. Les accès sont ponctuels et motivés par les tâches de ces personnes. Le conteneur de données consacré aux logues de plus de trois mois est en accès limité au RSSI et aux personnes désignées par le RSSI pour la mise en œuvre du droit d'accès aux intéressés et l'accès sur requête judiciaire.

La politique de sauvegarde de l'ensemble des données de l'établissement identifie les journaux contenant des données à caractère personnel dans le but de garantir leur suppression au delà d'une année.

Dans le cas d'une exploitation des journaux informatiques anonymisés, une copie anonymisée des logs est effectuée. L'anonymisation est réalisée dans le respect des règles de l'art, elle est irréversible. On se référera en particulier à l'expertise[3] publiée par la CNIL dans ce domaine.

Les intervenants

Les utilisateurs

Tous les utilisateurs, tels qu'ils sont définis en introduction de ce document, sont tenus de respecter la politique de sécurité et les chartes en vigueur dans l'établissement.

La chaîne fonctionnelle SSI

En dehors des acteurs de la chaine fonctionnelle rappelée ci-dessous, personne n'a de droit d'accès aux journaux informatiques comportant des données à caractère personnel, y compris la chaine hiérarchique. **Ils sont tenus au devoir de réserve ou de discrétion professionnelle, voire au secret professionnel**.

Les administrateurs systèmes et réseau

Ils sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau et veillent au respect des règles de sécurité des systèmes d'information. A ce titre, ils gèrent les traces dans le respect des obligations générales de leur fonction (politique de sécurité, chartes).

Ils rapportent, à leur supérieur dans la chaine fonctionnelle SSI, toute anomalie de fonctionnement ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur les systèmes ou le réseau.

Ils acceptent d'exécuter des traitements ou de fournir des informations pouvant inclure des données à caractère personnel uniquement à la demande de la chaine fonctionnelle de sécurité.

Les autres acteurs de la chaine fonctionnelle SSI :

- les correspondants de sécurité des systèmes d'information,
- le responsable de la sécurité des systèmes d'information (RSSI),
- l'autorité qualifiée de sécurité des systèmes d'information (AQSSI),
- le fonctionnaire de sécurité de défense (FSD).

3 http://www.cnil.fr/index.php?id=1536

Ils sont également tenus au devoir de discrétion professionnelle, et dans certains cas de secret professionnel en fonction de leur mission.

Les informations enregistrées

Informations journalisées par les serveurs (hors messagerie et Web) et postes de travail

Pour chaque tentative de connexion, d'ouverture de session de travail ou de demande d'augmentation de ses droits, tout ou partie des informations suivantes peuvent être enregistrées automatiquement par les mécanismes de journalisation du service :

- l'identifiant de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative (succès ou échec) ;
- les commandes passées.

Le choix d'une politique de centralisation des journaux informatiques des postes de travail peut être fait.

Services de messagerie, de messagerie instantanée, de forum et de listes de diffusion

Les serveurs hébergeant ces services mis en œuvre au sein de l'établissement enregistrent pour chaque message émis ou reçu tout ou partie des informations suivantes :

- l'adresse de l'expéditeur et éventuellement des éléments identifiant celui qui s'est connecté au serveur ;
- l'adresse des destinataires ;
- la date et l'heure de la tentative ;
- les différentes machines traversées par le message ;
- le traitement « accepté ou rejeté » du message ;
- La taille du message ;
- Certaines en-têtes du message, tel que l'identifiant numérique de message ;
- Le résultat du traitement des courriers non sollicités (spam) ;
- Le résultat du traitement antiviral éventuel;
- Les opérations de validation ou de rejet par les modérateurs quand cela s'applique.

Les éléments de contenu des messages ne sont pas journalisés, néanmoins, les applications peuvent

inclure des archives qui ne relèvent pas des journaux informatiques (chrono départ et réception).

Serveurs Web

On distingue les serveurs web exploités au sein de l'établissement et ceux situés en dehors de l'établissement.

Serveurs Web de l'établissement

Pour chaque connexion les serveurs Web enregistrent tout ou partie des informations suivantes en fonction des exigences de qualité de service et de sécurité de l'application web :

- les noms ou adresses IP source et destination ;
- les différentes données d'authentification dans le cas d'un accès authentifié (intranet par exemple) ;
- l'URL de la page consultée et les informations fournies par le client ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;
- les différents paramètres passés.

Serveurs Web hors établissement

Lorsque les utilisateurs sont des membres de l'établissement, pour chaque accès web via le réseau interne vers des serveurs externes peuvent être enregistrées tout ou partie des informations suivantes :

- les noms ou adresses IP source et destination et les différentes données d'authentification ;
- l'URL de la page consultée ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;

L'article L.34-1 du code des postes et des communications électroniques précise que les opérateurs de communications électroniques sont tenus à une obligation de conservation des données de connexion mais que celles-ci "ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ". Cette interdiction s'applique donc en particulier à l'URL des pages consultées dans le cas ou l'établissement offre des accès internet à des personnes extérieures à l'établissement.

En effet, il est alors possible d'assimiler le service réseau de l'établissement à celui d'un opérateur de communications électroniques.

La téléphonie sur IP

L'usage de la téléphonie sur IP peut engendrer des enjeux spécifiques dans le domaine de la sécurité ou dans celui du contrôle du bon fonctionnement des réseaux, mais bien entendu, les principes relatifs à la loi « Informatique et Libertés » s'appliquent à la téléphonie sur IP comme aux autres systèmes de téléphonie.

Lorsque des relevés justificatifs des numéros de téléphone appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés. Cependant, l'établissement peut éditer des relevés contenant l'intégralité des numéros appelés dans le cas où il demande aux personnels le remboursement du cout des communications personnelles ou dans celui où il a été constaté une utilisation manifestement anormale.

Le régime déclaratif de ces journaux fait l'objet de la norme simplifiée n 47[4] relative à l'utilisation de services de téléphonie fixe ou mobile sur les lieux de travail. En outre, la fiche pratique n 11 du guide « informatique et libertés » pour l'enseignement supérieur et la recherche [5] intitulée « Utilisation du téléphone sur le lieur de travail » détaille ce cas.

Les équipements réseau

On appelle « équipements réseau » les routeurs, pare-feu, commutateurs, bornes d'accès, équipement de métrologie et d'administration de réseau, etc. Pour chaque paquet qui traverse l'équipement tout ou partie des informations suivantes peuvent être collectées :

- les noms ou adresses IP source et destination ;
- les numéros de port source et destination ainsi que le protocole ;
- la date et l'heure de la tentative ;
- la façon dont le paquet a été traité par l'équipement ;
- le nombre de paquets et le nombre d'octets transférés ;
- les données d'authentification ;
- les messages d'alerte.

Les applications spécifiques

On entend par «applications spécifiques», toute application autre que celles mentionnées ci-dessus qui nécessite pour des raisons de comptabilité, de gestion, de sécurité ou de développement, l'enregistrement de certains paramètres de connexion et d'utilisation.

Parmi ces applications nous pouvons citer les exemples suivants :

- accès aux bases de données ;
- accès à l'ENT (espace numérique de travail) ;
- service d'authentification (SSO) ;

Comme dans le cas des serveurs web internes, des journaux génériques sont susceptibles d'être constitués et tout ou partie des informations suivantes peuvent être collectées :

- l'identifiant de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative ;
- les volumes de données transférées ;
- les commandes passées ;

Le traitement des logues décrit ici ne couvre pas l'ensemble des données conservées par ces applications qui de par leur nature peuvent historiser certaines transactions. Il est rappelé que si ces données visant à assurer la traçabilité des opérations ont un caractère personnel, elles sont alors soumises aux obligations de la loi Informatique et Libertés (déclaration auprès de la CNIL sauf en cas de désignation d'un Correspondant Informatique et Libertés (CIL), information préalable, etc)[6].

4 http://www.cnil.fr/index.php?id=1777
5 http://www.cnil.fr/fileadmin/documents/approfondir/dossier/education/Guide_InfoLib_Web.pdf
6 Le Correspondant Informatique et Libertés a été introduit en 2004 avec la réforme de la loi

Finalités des traitements effectués et leurs destinataires

Les traitements effectués doivent permettre d'obtenir des journaux qui répondent aux principes de base énoncés précédemment, tout en restant conformes aux obligations légales sur la protection des données à caractère personnel et de la vie privée.

Résultats statistiques

Ceux-ci sont effectués automatiquement et permettent de contrôler les volumes d'utilisation des moyens mis à la disposition des utilisateurs en temps qu'outil de travail. Lors de l'exploitation de ces résultats on s'attachera à distinguer les résultats anonymes de ceux qui peuvent être rapprochés de l'identité d'une personne. Parmi tous ces traitements on trouvera :

- des traitements statistiques en anonyme, en volume transféré et en nombre de connexions ;
- des classements des services les plus utilisés en volume de données et en nombre de connexions ;

Les résultats « anonymes » peuvent être conservés au-delà des délais mentionnés au paragraphe 3 et être diffusés sur des sites Internet accessibles à tous. Par contre, les administrateurs systèmes et réseau limitent l'accès aux résultats contenant des données à caractère personnel à eux-mêmes et éventuellement à la chaine fonctionnelle SSI. La durée de conservation de ces statistiques non anonymisées ne peut excéder celle des journaux utilisés pour produire ces statistiques.

Résultats d'analyse

La politique de sécurité, applicable à chaque ressource informatique qui génère des traces, définit des règles d'analyse systématique de ces traces afin de pouvoir détecter, dans les meilleurs délais, les incidents relatifs à la sécurité des systèmes d'information.

En cas d'incident, des analyses peuvent être faites par les administrateurs systèmes et réseau sur les traces disponibles. Les résultats ne peuvent être transmis qu'à la chaine fonctionnelle SSI et au CERT-Renater ou CERTA pour les incidents de sécurité.

Dans ce cas, l'accès aux trafics et aux traces est limité aux exploitants des systèmes en charge d'analyser l'incident et au RSSI. L'extraction de l'information et son utilisation sont strictement limitées à l'analyse de l'incident. Si l'incident n'est pas avéré les résultats sont non transmis et immédiatement détruits.

Détection des usages abusifs

On entend ici par « usages abusifs » les usages du réseau qui sont contraires aux lois, règlement intérieur ou chartes d'usage des moyens informatiques. Sont aussi visés les usages qui compromettent les services du réseau de l'établissement (consommation excessive de bande passante, introduction de faille dans la sécurité du réseau, etc).

Les logues peuvent être exploités pour mettre en évidence ces abus. Par exemple, des classements des machines ayant consommé le plus de réseau en volume transféré et en nombre de

---

informatique et libertés. Sa désignation permet d'être exonéré de l'obligation de déclaration préalable des traitements ordinaires et courants. Seuls les traitements identifiés comme sensibles dans la loi demeurent soumis à autorisations et continuent à faire l'objet de formalités. Il a un rôle de conseil et suivi dans la légalité de déploiement des projets informatiques et, plus largement, de la gestion de données à caractère personnel.

connexions permettent souvent de détecter l'utilisation indésirable de protocoles de peer to peer ou la présence de serveurs pirates. Se référer à la fiche pratique « Contrôle de l'utilisation des moyens informatiques » du guide pratique « Informatique et Libertés » pour l'enseignement supérieur et la recherche.

Quand ils sont mis en œuvre, ces traitements le sont de façon systématique (ils sont appliqués à toutes les machines du réseau de l'établissement ou d'une partie donnée du réseau) et ne ciblent aucune personne ou catégorie de personnes.

Des journaux bruts

Ceux-ci permettent de replacer une action particulière dans son contexte, à des fins d'enquête. Dès l'apparition d'un incident, les journaux bruts pourront être requis par la chaine fonctionnelle.

Les administrateurs systèmes et réseau sont chargés de l'application de la requête, et ils sont, pour cette activité, soumis au secret professionnel.

Les journaux bruts sont remis, à sa requête à l'autorité judiciaire afin de lui permettre de poursuivre une enquête.

Droit d'accès individuel

Chaque agent peut demander à consulter les traces qui le concernent. Les demandes doivent être faites par écrit auprès du directeur de l'entité d'hébergement.

La recherche est faite par l'administrateur, sur demande de sa hiérarchie, et les résultats sont transmis directement à l'utilisateur demandeur, sous la forme d'un «courrier personnel».

Informations des utilisateurs sur la politique de gestion des journaux informatiques

L'établissement doit informer ses utilisateurs de la gestion qui est faite des traces qui les concernent. Cela sera fait par la diffusion systématique de ce document qui sera référencé dans la charte informatique de l'établissement. Ce document sera rendu accessible à tout utilisateur par le réseau. Il pourra être mis en valeur dans l'intranet de l'établissement ou par voie d'affichage. Une attention particulière sera portée à la publicité de ce document lors de la mise à disposition de nouveaux services concernés par les journaux informatiques ainsi qu'auprès des nouveaux utilisateurs des moyens informatiques de l'établissement[7].

Une information et une consultation préalable des instances représentatives des personnels doit être prévue.

7 Se reporter au guide pratique de la CNIL à l'attention des employeurs, sections "cybersurveillance sur le lieu de travail", "le contrôle de l'usage de la messagerie électronique", "le rôle des administrateurs informatiques" .