PROCÉDURE DE MISE EN CONFORMITÉ

à la loi informatique et libertés

DIFFUSION	Restreinte à l'UCBN
RÉFÉRENCE	PRO-IetL-MEC-V1.0

	Prénom/Nom	Entité	Date
RÉDACTION	François GIRAULT	UCBN	15/02/11
RELECTURE	• Véronique BUDET • Annie COBALTO	UNR-RUNN UCBN-CRISI	31/01/12

Historique des mises à jour			
Date	**Modification demandée par**	**Description du changement**	**Version**
02/03/12	François Girault	Corrections mineures	1.0

Table des matières

1. Objet

Cette procédure indique les différentes étapes afin de réaliser la mise en conformité avec la loi Informatique et Libertés d'une composante, d'une structure ou d'un service de l'Université de Caen Basse-Normandie.

Cette mise en conformité est composée de deux étapes.
La première permettant de :

- référencer l'ensemble de traitements de données à caractère personnel et de s'assurer de la licéité de ces traitements.
- sensibiliser les personnels de la composante, de la structure ou du service afin de leur faire prendre conscience de ce qu'est la législation en matière d'Informatique et Libertés, des obligations de chacun et des risques encourus par l'établissement.

La seconde étape permet de réaliser la mise en conformité effective de l'établissement à la loi Informatique et Libertés par l'inscription au registre des traitements ainsi que la modification éventuelle de ceux-ci s'il s'avère qu'ils ne sont pas conformes.

Cette procédure de mise en conformité n'est pas un audit au sens de la norme NF ISO-19011 mais une étape préliminaire permettant de dresser un état des lieux de l'application de la loi Informatique et Libertés au sein de l'établissement.

2. Domaine d'application

Cette procédure s'applique à toutes les composantes, structures et services de l'Université de Caen Basse-Normandie. Elle peut s'appliquer totalement ou partiellement suivant les besoins.

Par exemple :

- Application totale de la procédure pour la mise en conformité initiale des composantes, structures et services de l'Université de Caen Basse-Normandie.
- Application partielle lors des entretiens individuels des nouveaux venus dans une composante, structure ou service.

Afin de n'oublier aucune structure de l'Université de Caen Basse-Normandie, cette procédure s'applique à toutes les structures et sous-structures référencées comme indiquées sur les pages web de l'université [1] et pour lesquelles l'Université est considérée comme responsable de traitements. Les structures hébergées (celles dont l'identifiant de structure est préfixé par Y), seuls les transferts entre l'Université et la structure sont référencés.

3. Intervenants

Cette procédure peut être menée par le CIL de l'Établissement, par le CSSI de la composante ou du service ou conjointement par le CIL de l'établissement et par le CSSI de la composante ou de la structure.

Dans le cas où cette procédure est appliquée par le CSSI de la composante ou du service, l'entretien collectif n'est pas nécessaire, il sera réalisé ultérieurement par le CIL. Concernant les entretiens individuels, Il n'est demandé qu'un référencement des traitements et des données collectées. Ces informations seront ensuite transmises au CIL qui vérifiera la licéité du traitement ainsi que l'adéquation des données collectées avec la finalité déclarée.

[1] https://gest.unicaen.fr/outils/index.php?page=ss_struct

4. Définitions

Audit : Processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure des critères prédéterminés sont satisfaits (d'après NF ISO19011).

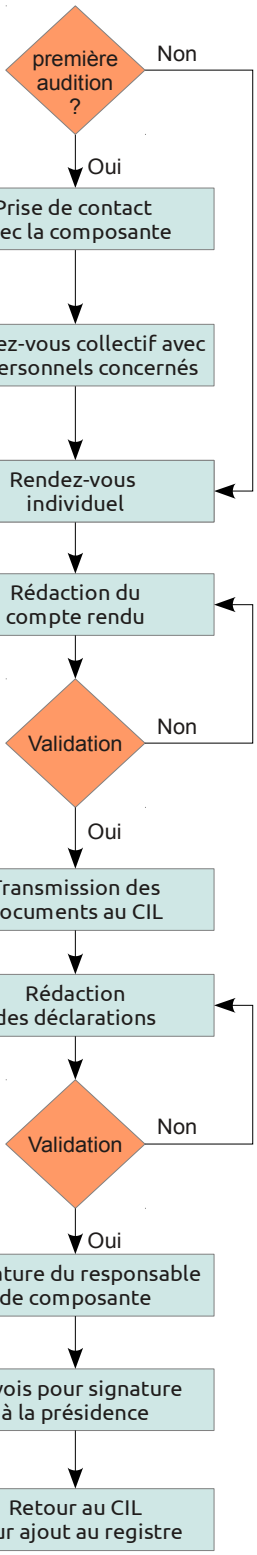
Audit « Informatique et Libertés » : Un audit « Informatique et Libertés » est un audit dont les critères permettent de juger de la conformité de traitements de données à caractère personnel à la loi n° 8-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiées par la loi n° 2004-801 du 6 août 2004 (d'après délibération n° 2011-316 du 6 octobre 2011 – NOR : CNIA1100014X)

Donnée à caractère personnel : Donnée permettant d'identifier directement ou indirectement un individu (d'après loi 78-17 modifiée 2004-801).

Loi Informatique et Libertés : loi française promulguée à la suite de l'affaire SAFARI, et qui réglemente aujourd'hui notamment la pratique du fichage, manuel ou informatique.

5. Logigramme

QUI	FAIT QUOI	COMMENT
Correspondant I&L	Prise de contact avec la composante	Par mail
CIL, CSSI, Responsable de la composante et les personnels concernés	Rendez-vous collectif avec les personnels concernés	Exposé didactique et échange questions/réponses
CIL et/ou CSS ainsi que chaque personne du service ou de la composante.	Rendez-vous individuel	Présentation du travail, mise en situation
CIL ou CSSI	Rédaction du compte rendu	À partir des prises de notes des entretiens individuels
La personne interviewée individuellement	Validation	
La personne interviewée individuellement	Transmission des documents au CIL	
CIL ou CSSI	Rédaction des déclarations	
La personne interviewée individuellement ou le CIL (si rédaction par CSSI)	Validation	
Responsable de la composante, du service ou de la structure	Signature du responsable de composante	
Correspondant Informatique et Libertés	Envois pour signature à la présidence	
Présidence de l'Université	Retour au CIL pour ajout au registre	



Note : Ce logigramme ne contient pas la partie récurrente de l'audit à savoir le rappel annuel des traitements déclarés.

6. Descriptif de la procédure

6.1. Prise de contact avec la composante

Il est tout d'abord primordial de contacter le directeur ou le responsable administratif de la composante, de la structure ou du service afin de l'informer de l'existence de l'audit et d'expliciter succinctement les objectifs de celui-ci puis de convenir d'un rendez-vous avec l'ensemble du personnel administratif pouvant être amené à manipuler des données à caractère personnel.

6.2. Rendez-vous avec les personnels concernés

Le rendez-vous avec les personnels concernés permet de faire une sensibilisation au respect de la loi Informatique et Libertés. Il est souhaitable que le CSSI soit présent. Lors de cet entretien collectif, le CIL présente la loi, les obligations du responsable des traitements ainsi que des cas concrêts concernant la composante auditée. Ensuite vient une période de libre échange ou chacun pose des questions relatives aux traitements qui sont en cours.
Cette période d'échange permet de s'assurer que les personnels présents ont bien compris les tenants et aboutissants de la loi et la manière de rendre un traitement licite.
En fin de réunion, rendez-vous est pris avec chaque personnel ou petit groupe de personnel (maximum 3 pers.) afin d'effectuer l'entretien individuel. Le détail de la procédure d'entretien collectif est décrit dans la procédure PRO-IetL-EntretienCollectif.

6.3. Entretien individuel

Lors de l'entretien individuel, le personnel interviewé explique en détail ses missions et son travail. L'accent est bien évidemment porté sur le traitement des données à caractère personnel. Ces traitements sont catégorisés en fonction de leur finalité et des destinataires (tant internes à l'établissement qu'externes). Ces traitements sont référencés sur la fiche « Compte rendu d'audit informatique et Libertés » qui permettra de remplir les demandes d'inscription au registre.
Le détail de la procédure d'entretien individuel est décrit dans la procédure PRO-IetL-EntretienIndividuel

6.4. Déclaration des traitements

Une fois l'entretien individuel réalisé, le compte rendu est envoyé au personnel interviewé avec pour objectif de vérifier que le compte rendu correspond en tout point à ce qui a été mentionné. Dans ce compte rendu, il est aussi demandé de retourner pour chaque traitement réalisé une copie des documents traités. Une fois les documents reçus, le CIL remplit la demande d'inscription au registre et la renvoie au personnel interviewé pour signature par le responsable de la composante.

Une fois la demande d'inscription au registre signée elle est envoyée à la Présidence pour signature et est ensuite inscrite au registre de l'établissement.

6.5. Rappel annuel

La mise en conformité de l'établissement est un processus récurrent d'amélioration perpétuelle. Tous les ans les composantes ayant inscrit des traitements au registre informatique et libertés reçoivent un récapitulatif des traitements déclarés. Il est demandé d'indiquer toute modification de traitement mais aussi tout nouveau traitement ou tout traitement ayant cessé. Si de nouvelles personnes ont intégré la composante, la structure ou le service, un entretien est proposé afin de faire un rappel à la loi Informatique et Libertés.

7. Annexes

7.1. Matrice d'un rapport d'entretien individuel

Compte rendu d'entretien individuel Informatique et Libertés CR-IetL-EntretienIndividuel-V1.1

université de Caen Basse-Normandie

Compte rendu d'entretien individuel Informatique et Libertés

Structure
Sous Structure
Présents •

Date d'entretien

1. Rappels sur la Loi Informatique et Libertés

Historique de la Loi Informatique et Libertés :

- ☐ Projet SAFARI
- ☐ Création de la CNIL
- ☐ Loi de 1978
- ☐ Loi de 2004

Définitions :

- ☐ Donnée à caractère personnel
- ☐ Identification
- ☐ Traitement
- ☐ Responsable de traitement

Les types de déclaration :

- ☐ Normale
- ☐ Simplifié
- ☐ Déclaration de conformité
- ☐ Demande d'avis
- ☐ Demande d'autorisation

Les lois connexes :

- ☐ CADA
- ☐ Archivage
- ☐ Code de santé publique
- ☐ Code de l'éducation

Les 5 règles d'or :

- ☐ Respect de la finalité
- ☐ Pertinence des données
- ☐ Durée de conservation limitée
- ☐ Obligation de sécurité
- ☐ Respect du droit des personnes

2. Description des traitements

2.1 Traitement 1 :

Description détaillée du traitement :

Tableau récapitulatif :

Finalité	
Données traitées	
Durée de conservation	
Destinataires internes	
Destinataires externes	
Documents associés	

Remarques :

Diffusion restreinte UCBN contact : cil@unicaen.fr 1/1 Modèle version 1.1 (modifié le 13/01/2012)

7.2. Matrice d'un rapport d'entretien collectif

université de Caen Basse-Normandie

Compte rendu d'entretien collectif Informatique et Libertés

Structure
Sous Structure
Présents •

Date d'entretien

1. Rappels sur la loi Informatique et Libertés

Historique de la Loi Informatique et Libertés :

- ☐ Projet SAFARI
- ☐ Création de la CNIL
- ☐ Loi de 1978
- ☐ Loi de 2004

Définitions :

- ☐ Donnée à caractère personnel
- ☐ Identification
- ☐ Traitement
- ☐ Responsable de traitement

Les types de déclaration :

- ☐ Normale
- ☐ Simplifié
- ☐ Déclaration de conformité
- ☐ Demande d'avis
- ☐ Demande d'autorisation

Les lois connexes :

- ☐ CADA
- ☐ Archivage
- ☐ Code de santé publique
- ☐ Code de l'éducation

Les 5 règles d'or :

- ☐ Respect de la finalité
- ☐ Pertinence des données
- ☐ Durée de conservation limitée
- ☐ Obligation de sécurité
- ☐ Respect du droit des personnes

2. Tour de table

Présentation détaillée des fonctions de chacun :

Nom	Prénom	Fonction

3. Session Questions/Réponses

Question :

Réponse :

4. Remarques et commentaires