POLITIQUE DE SÉCURITE
DES SYSTÈMES D'INFORMATION
Version 1.0

HISTORIQUE DES VERSIONS		
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**
31/10/2013	1.0	Version originale
10/07/2019	1.1	Remise en forme avec la nouvelle charte graphique

TABLE DES MATIERES

1. Avant-propos

1.1. Objectifs de la PSSI

Les systèmes d'information sont le socle de nombreuses activités critiques liées à toutes les missions de l'université de Tours. Les systèmes d'information constituent une valeur ajoutée devant contribuer à l'excellence et aux défis de l'université d'aujourd'hui et de demain (enseignement à distance, ENT, ...).

La Politique de Sécurité des Systèmes d'Information est le document de référence pour l'université de Tours qui énonce les règles opérationnelles de sécurité qui doivent être implémentées.

Ces règles découlent des mesures sélectionnées en réponse aux risques évalués sur l'ensemble du périmètre de l'Université de Tours.

1.2. Périmètre

La PSSI s'applique à l'ensemble du système d'information de l'Université de Tours.

Par "Système d'Information", il faut comprendre l'ensemble des moyens mis en œuvre par l'Université de Tours pour opérer les services nécessaires à ses missions et qui traitent les informations de Gestion, d'Enseignement et de Recherche. Ainsi, au-delà des matériels informatiques, des logiciels et des données manipulées, la PSSI définit aussi des règles de sécurité relatives à l'organisation, aux personnes opérant ces systèmes et à leurs infrastructures d'accueil.

2. Gestion de la politique de sécurité

2.1. Organisation pour la gestion de la SSI

Une politique de management de la sécurité de l'Information décrit les processus et les rôles et responsabilités des intervenants en matière de gestion de la sécurité. Cette politique de management est décrite dans le document [1].

Un Comité de Sécurité Opérationnelle est mis en place au sein de l'Université de Tours, afin de coordonner les activités liées à la sécurité, de relayer les décisions du Comité de Pilotage Stratégique et de lui fournir la visibilité nécessaire sur l'état des lieux de la sécurité du système d'information en regard des règles de la PSSI.

2.2. Mise en œuvre de la politique de sécurité

La présente Politique de Sécurité est rédigée sous la responsabilité du Comité de Pilotage et fait suite au projet national de Politique Générale de Sécurité des Systèmes d'Information. La stratégie de traitement des risques retenues et les règles de sécurité en résultant doivent être mises en œuvre, appliquées et contrôlées par les intervenants concernés.

2.3. Approbation et Diffusion

La PSSI est approuvée par le président de l'Université de Tours. C'est un document à diffusion restreinte à l'Université de Tours et à certains de ses partenaires. Elle est diffusée à tout le personnel de l'Université de Tours ayant le besoin d'en connaître.

2.4. Contrôle et suivi

Des contrôles de mise en œuvre opérationnelle et d'efficacité des règles de sécurité énoncées peuvent être réalisés.

2.5. Gestion des évolutions

Le Comité de Sécurité Opérationnelle procède à la mise à jour de la PSSI en fonction des évolutions du système d'information, des besoins de sécurité, et des risques identifiés.

2.6. Relation avec les autorités

La gestion de la sécurité doit couvrir et définir les relations à établir avec les autorités compétentes et notamment sur les aspects suivants :

- Respect des lois et réglementations
- Remontées en cas d'incidents de sécurité grave (ANSSI et CERT)
- Gestion des données personnelles (CNIL)
- Respect de la Charte de bon usage de l'informatique et du reseau RENATER

3. Orientations générales

3.1. Lignes directrices

L'Université de Tours se doit de protéger son patrimoine informationnel face aux risques pouvant impacter ses orientations stratégiques, ou pouvant affecter la réalisation de ses missions. La PSSI doit concourir à l'atteinte des objectifs de l'Établissement à savoir :

- Développer l'insertion professionnelle
- Conforter la recherche
- Développer la vie étudiante
- Améliorer l'enseignement
- Optimiser le fonctionnement de l'université
- Favoriser le développement durable

3.2. Exigences légales

Chaque établissement est responsable de ses données et doit appliquer les lois et règlements en vigueur.

3.3. Sensibilisation et formation

La formation et la sensibilisation des personnes à la sécurité de l'information constituent un maillon essentiel de la sécurité. Ainsi, le service des Ressources Humaines organise régulièrement des sessions de formation ou de sensibilisation adaptées aux besoins des différents usagers : agents, chercheurs, enseignants, étudiants, personnels des services informatiques, en coopération avec la DSI. Un plan annuel de formation est proposé par le Comité de Sécurité Opérationnelle.

4. Gestion des biens

4.1. Classification des biens

Il convient de classer les informations en termes de valeur, d'exigences légales, de sensibilité et de criticité.

4.2. Inventaire des biens

Il convient de clairement identifier tous les biens, de réaliser et de gérer un inventaire de tous les biens importants.

4.3. Marquage des biens

Il convient d'élaborer et de mettre en œuvre un ensemble approprié de procédures pour le marquage et la manipulation de l'information, conformément au plan de classification adopté par l'organisme.

4.4. Propriété des biens

Il convient d'attribuer la propriété de chaque information et moyens de traitement de l'information à une partie définie de l'organisme. Il convient d'identifier, de documenter et de mettre en œuvre des règles permettant l'utilisation correcte de l'information et des biens associés aux moyens de traitement de l'information.

Il convient d'établir des procédures de manipulation et de stockage des informations pour protéger ces informations d'une divulgation non autorisée ou d'un mauvais usage.

5. Sécurité liée aux ressources humaines

5.1. Responsabilités des utilisateurs

5.1.1. Responsabilités génériques

La charte d'usage et de sécurité des systèmes d'information, destinée aux différentes populations utilisatrices du système d'information (personnels administratifs, enseignants, chercheurs, et étudiants de l'Université de Tours), précise les droits, devoirs et responsabilités qui incombent à tout utilisateur du système d'information en matière de sécurité.

Elle est diffusée pour signature à tous les nouveaux arrivants. La charte est accessible depuis la page web de l'université, depuis l'aide de l'ENT ainsi que depuis les pages d'authentification des réseaux Wifi.

5.1.2. Manquement aux exigences

Les chartes utilisateurs définissent les conditions d'usage du système d'information en termes de sécurité.

Les chartes informent les utilisateurs des contrôles effectués et mentionne le processus disciplinaire (rappel aux bonnes pratiques, sanction administrative, poursuite pénale...) mis en œuvre en cas de d'infraction aux règles de sécurité.

5.2. Formation et sensibilisation du personnel

5.2.1. Information du personnel

Les droits, les devoirs et les responsabilités associées à chaque poste en matière de Sécurité du Système d'Information sont communiqués à toute personne lors de sa prise de fonction ou d'un changement de poste.

Un document (charte ou procédure), disponible à chaque membre du personnel, l'informe des consignes de sécurité à respecter dans le cadre des tâches qu'il exécute au sein de l'Université de Tours.

L'information du personnel concerne à la fois les personnels de l'Université de Tours (personnels administratifs, les enseignants, les chercheurs), mais aussi les étudiants, tiers et contractants.

5.2.2. Sensibilisation des personnels

Il est important que chaque personne impliquée dans le traitement d'informations sensibles de l'Université de Tours soit sensibilisée aux enjeux de « sécurité » et soit formée de manière à pouvoir gérer les mesures de sécurité qui lui incombent.

Des sessions d'information à la sécurité sont assurées périodiquement afin de maintenir la sensibilisation des personnels administratifs, enseignants, chercheurs, et étudiants, sur les bonnes pratiques de sécurité ou sur les règlements en vigueur.

Des formations spécifiques sont réalisées pour les personnels dont les fonctions requièrent une sensibilisation particulière en termes de sécurité (personnels liés à la DSI, chercheurs).

5.3. Disponibilité des personnels critiques

Une gestion adaptée des ressources humaines est mise en place de manière à ce qu'il n'y ait pas de vacance sur un poste critique qui puisse impacter la sécurité, ou induire une indisponibilité incompatible avec les objectifs de sécurité retenus. Il convient en particulier que les ressources affectées soient en cohérence avec les objectifs en matière de disponibilité.

5.4. Suivi des biens, ressources et autorisations allouées

5.4.1. Gestion des biens et autorisations alloués aux personnes

Les biens sensibles (badges, équipements...) et les autorisations (accès aux locaux, aux données et fonctions du SI...) alloués à chaque personne sont gérés et suivis.

Une procédure définit la gestion et le suivi des matériels sensibles alloués aux personnes de l'Université de Tours et aux contractants, et des autorisations (informations, sites, badges...) qui leurs sont délivrées.

La procédure définit également les conditions d'allocation des biens en fonction des besoins.

5.4.2. Gestion des biens en fin de contrat

La procédure de suivi des matériels sensibles définit les conditions de restitution des biens (fin de contrat, changement de poste).

6. Gestion des tiers

6.1. Identification des risques liés aux relations avec des tiers

Toute interconnexion entre le SI de l'Université de Tours et le SI d'un tiers (ou laboratoire) fait l'objet d'une étude pour valider les besoins, identifier les risques, et définir les mesures de sécurité complémentaires à mettre en œuvre par l'Université de Tours ou par le tiers.

6.2. Sécurité liée aux accès clients

Lorsqu'une relation de type client / fournisseur est établie entre l'Université de Tours et un organisme ou une personne externe (échanges d'information avec des laboratoires, avec des étudiants), les besoins de sécurité sont étudiés avant l'ouverture d'un accès à l'information ou aux biens de l'Université de Tours.

6.3. Prise en compte de la sécurité dans les relations contractuelles

Des accords de confidentialité et annexes de sécurité spécifiant les éléments couverts par ces accords sont établis dès les phases précontractuelles. Ces éléments, mis à jour si nécessaire lors de la contractualisation, sont annexés au contrat signé avec les tiers. Des dispositions particulières définissent les points à prendre en compte lors de la clôture du contrat afin de garantir la sécurité du SI de l'Université de Tours postérieurement à celui-ci.

Notamment : Tout marché public impliquant des moyens du système d'information est validé et le cas échéant complété par le RSSI (y compris pour des maintenances à distance, la gestion des supports numériques lors de dépannage ou échanges standards).

6.4. Prestation de services par un tiers

Les obligations en matière de sécurité relatives aux services fournis par des tiers et au niveau de prestation attendu sont formalisées, généralement dans le cahier des charges de la prestation. Ces obligations sont mises en œuvre, appliquées et tenues à jour conformément à ce qui est défini par les accords contractuels.

6.5. Surveillance et examen des services tiers

Les services fournis par des tiers sont régulièrement contrôlés et évalués. À ce titre, les prestataires fournissent à la DSI des rapports et enregistrements suffisants pour permettre ce contrôle et cette évaluation.

L'existence et les modalités de cet examen périodique sont précisées dans les contrats ou conventions conclues avec les tiers.

Les modalités de contrôle et d'audit sont définies, telle la fourniture d'éléments supports au responsable du suivi de la prestation ou au responsable de l'audit.

6.6. Gestion des modifications dans les services tiers

Les changements effectués dans la prestation de service des tiers sont suivis et formalisés.

L'évolution du système d'Information, des besoins de sécurité ou l'identification de nouveaux risques peuvent notamment apporter des changements au niveau des services tiers.

7. Sécurité physique et environnementale

7.1. Structuration de l'infrastructure en zones de confiance

7.1.1. Définition des périmètres de sécurité physique

Il convient de protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité (obstacles tels que des murs, des portes avec un contrôle d'accès par cartes, ou des bureaux de réception avec personnel d'accueil).

7.1.2. Contrôle physique des accès

Il convient de protéger les zones sécurisées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis.

7.1.3. Choix de l'emplacement et protection du matériel

Il convient de situer et de protéger le matériel de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.

7.1.4. Travail dans les zones sécurisées

Il convient de concevoir et d'appliquer des mesures de protection physique et des directives pour le travail en zone sécurisée.

7.2. Contrôle physique des accès

7.2.1. Contrôle des accès physiques, gestion des autorisations

Il convient de protéger les zones sécurisées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis.

7.2.2. Sécurisation des bureaux, des salles et des équipements

Il convient de concevoir et d'appliquer des mesures de sécurité physique pour les bureaux, les salles et les équipements.

7.3. Contrôle physique des accès

7.3.1. Accueil et accompagnement des visiteurs

Il convient de protéger les zones sécurisées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis.

7.3.2. Zones d'accès publiques, de livraison et de chargement

Il convient de contrôler les points d'accès tels que les zones de livraison/chargement et les autres points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux. Il convient également d'isoler les points d'accès, si possible, des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

7.4. Sortie des matériels

7.4.1. Sécurité du matériel hors des locaux

Il convient d'appliquer la sécurité au matériel utilisé hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site.

7.4.2. Sortie d'un matériel

Il convient de ne pas sortir un matériel, des informations ou des logiciels des locaux de l'organisme sans autorisation préalable.

7.5. Mise au rebut sécurisée

7.5.1. Destruction des biens sensibles

Les procédures de mise au rebut des biens sensibles sont formalisées et communiquées à l'ensemble du personnel présentant un besoin d'en connaître.

La mise au rebut des supports papiers contenant des informations sensibles est réalisée au moyen d'une déchiqueteuse ou d'incinérateurs. La conservation des documents est effectuée en lieu sûr avant leur destruction.

La mise au rebut des supports électroniques est réalisée de manière sécurisée : par effacement sécurisé, par broyage, incinération ou par enlèvement par une société spécialisée. La conservation des matériels est effectuée en lieu sûr avant destruction.

7.6. Protection contre les menaces extérieures et environnementales

7.6.1. Localisation des matériels

Les matériels du système d'information, présentant une valeur attractive, fragiles, ou supports d'information sensibles sont disposés dans des emplacements appropriés garantissant leur sécurité (imprimantes, vidéoprojecteurs, ordinateurs libre-service, serveur de données, etc.). Notamment ces matériels sont entreposés dans des salles ou armoires fermées à clés en absence des personnes responsables, disposent d'équipement antivol, de marquage indélébile en empêchant la revente, etc.

7.7. Équipement d'infrastructure du site

7.7.1. Adéquation des équipements d'infrastructure

Tout local dédié aux équipements informatiques et réseaux dispose d'infrastructures nécessaires au fonctionnement des moyens informatiques du site et à leur sécurité : climatisation (climatiseurs, arrivées d'eau...), équipements de protection incendie (sprinklers, extincteurs...), alimentation électrique (onduleurs, groupes électrogènes, arrivées électriques...), moyens de télécommunication (PABX, lignes...).

Le dimensionnement des équipements d'infrastructure mis en œuvre permet d'assurer le bon fonctionnement des moyens informatiques et réseaux du site comme de leur sécurité.

7.7.2. Redondance des équipements d'infrastructure

Les équipements d'infrastructure du site présentent un niveau de redondance suffisant pour assurer un bon fonctionnement de l'infrastructure et des moyens informatiques.

7.7.3. Maintenance des équipements d'infrastructure

Les équipements d'infrastructure sont couverts par des contrats de maintenance et si nécessaire par des contrats de services permettant d'assurer la disponibilité du service rendu par ces équipements.

7.7.4. Protection des câbles

Les salles informatiques disposent de faux planchers ou de goulottes appropriées permettant un passage sécurisé des différents câblages.

8. Habilitation et contrôle d'accès logique

8.1. Gestion des habilitations

8.1.1. Gestion des profils et des droits alloués

Une procédure de gestion des habilitations définit les principes de gestion des profils et des droits correspondants en termes d'accès aux ressources du système d'information. La gestion des habilitations concerne les chercheurs, enseignants, étudiants, agents administratifs par métier.

Cette procédure couvre la création, la modification et la suppression des comptes de l'utilisateur, et donc des droits associés à ses profils.

Les droits alloués à chaque profil sont limités aux seuls droits nécessaires à l'accomplissement des missions qui incombent aux titulaires de ce profil.

La liste des profils et des droits alloués à chaque profil est tenue à jour. Les profils comme les droits alloués sont périodiquement révisés.

8.1.2. Demandes concernant les habilitations et droits d'accès

Il convient de restreindre et de contrôler l'attribution et l'utilisation des privilèges.

8.1.3. Validation des demandes concernant les habilitations et droits d'accès

Il convient que le responsable de l'application ou des données pour lesquelles des droits sont demandés valide chaque demande préalablement à l'ouverture des droits.

Un processus de demande est défini et adapté à chaque profil, pour la validation d'accès aux ressources demandées. L'historique de ces validations de demandes doit être conservé.

8.1.4. Suivi et révision des habilitations et droits d'accès

Des revues formalisées des profils et des droits d'accès associés ainsi que des habilitations (utilisateurs auxquels les profils sont attribués) ont lieu périodiquement. Ces revues visent à supprimer les éventuels accès inappropriés.

Ces revues sont menées par les responsables d'application.

8.1.5. Retrait des habilitations et droits d'accès

Un processus de retrait des droits d'accès est défini selon les profils (en particulier révisé pour les agents à chaque changement de poste ou de fonction).

Les droits d'accès des étudiants sont systématiquement supprimés en fin de cycle d'enseignement.

8.2. Droits d'accès

8.2.1. Identification et authentification

Les utilisateurs des applications et des serveurs sont identifiés individuellement, de manière unique et normalisée. A chaque identifiant est associé un authentifiant respectant les exigences stipulées en la matière.

8.2.2. Gestion des comptes

Un processus formel décrit la manière dont les comptes utilisateurs sont gérés, et en particulier comment ils sont créés, modifiés ou supprimés, selon les applications et les profils. Les règles de diffusion des identifiants et authentifiants aux utilisateurs sont aussi formalisées.

8.2.3. Caractéristiques des comptes

Tout compte permet d'identifier son titulaire.

Les identifiants respectent la codification interne de l'Université de Tours.

8.2.4. Caractéristiques des authentifiants

Lorsque des mots de passe sont utilisés comme authentifiants, ils respectent les règles de bonnes pratiques

Pour les personnels : Annuaire OpenLDAP

- Durée de vie : 1 an
- Longueur minimale : 8 caractères
- Complexité : 1 numérique et 1 majuscule minimum
- Comparaison avec un dictionnaire et interdiction du nom et/ou prénom
- Historique de réutilisation : 2
- Blocage après 15 tentatives sur 10 minutes
- Temps de grâce de 10 minutes

Pour les personnels : Annuaire Active Directory et applications

- Durée de vie : 1 an
- Longueur minimale : 8 caractères
- Complexité : 1 numérique et 1 majuscule minimum
- Historique de réutilisation : 2
- Blocage après 10 tentatives sur 10 minutes
- Temps de grâce de 10 minutes

Pour les étudiants : Annuaire OpenLDAP

- Durée de vie : illimité
- Longueur minimale : 8 caractères

- Complexité : 1 numérique et 1 majuscule minimum
- Comparaison avec un dictionnaire et interdiction du nom et/ou prénom
- Historique de réutilisation : 2
- Blocage après 15 tentatives sur 10 minutes
- Temps de grâce de 10 minutes

Pour comptes à privilèges élevés :

- Durée de vie : 6 mois (illimité pour les comptes d'automatisation
- Tel que les scripts ou les services)
- Longueur minimale : 12 caractères
- Complexité : 1 numérique + 1 majuscule +1 caractère spécial minimum
- Historique de réutilisation : 2

8.2.5. Confidentialité des authentifiants

Des mesures garantissent la confidentialité des authentifiants circulant sur le réseau (utilisation de protocoles sécurisés, réseau d'administration isolé).

Il est régulièrement rappelé aux utilisateurs qu'ils doivent protéger leurs mots de passe et ne les communiquer à personne.

Par "système de gestion de mots de passe", il faut entendre toutes les fonctions, intégrées dans les applications ou les systèmes, ou dédiés à la sécurité, prenant en charge l'authentification des utilisateurs.

8.2.6. Systèmes de gestion des mots de passe

Les logiciels ou fonctions utilisés pour générer ou contrôler les mots de passe choisis par l'utilisateur répondent aux exigences définies dans le présent document. Les mots de passe ne répondant pas aux exigences doivent être refusés par le système.

Les mots de passe sont stockés de façon sécurisée par la mise en œuvre de mécanismes cryptologiques.

8.3. Suivi des accès

8.3.1. Suivi des accès

Tous les accès aux données sensibles et fonctions sensibles sont tracés et sont régulièrement analysés et contrôlés.

Les traces sont sauvegardées et conservées de façon sécurisée pendant une période de temps suffisante pour répondre aux besoins opérationnels et satisfaire les exigences réglementaires.

8.3.2. Traitement des comptes inactifs

Les comptes individuels non utilisés pendant 6 mois sont désactivés.

Sauf cas particuliers (longue maladie, détachement, ...), les comptes désactivés sont supprimés au bout de 90 jours.

Sauf cas particuliers (retraités, etc.), les comptes des personnes ayant quitté l'Université de Tours sont supprimés.

8.4. Gestion des comptes privilégiés

8.4.1. Gestion des comptes privilégiés

Les comptes privilégiés et les droits alloués à ces comptes sont réservés aux administrateurs et aux exploitants. Une liste écrite des administrateurs et exploitants ayant accès aux comptes privilégiés, est établie et maintenue à jour. Pour tout compte privilégié partagé, cette liste indique le responsable identifié et la liste des personnes ayant accès à ce compte.

8.4.2. Gestion des comptes système génériques ou partagés

Rentrent dans cette catégorie les comptes tels que « root » sous Unix ou « Administrateur » sous Windows, les comptes dédiés à l'administration de progiciels... L'utilisation de tels comptes peut s'avérer indispensable pour réaliser certaines opérations d'administration et de supervision.

Chaque compte a un ou plusieurs titulaire(s) responsable(s) identifié(s).

Le titulaire a en charge la gestion du mot de passe du compte.

L'utilisation des comptes privilégiés partagés est limitée au strict nécessaire. L'utilisation de comptes système personnels est privilégiée.

Si un compte système est utilisé par une autre personne que le titulaire ou un utilisateur accrédité, l'utilisation se fait en présence du titulaire du compte ou d'une personne qualifiée pour le représenter. Le mot de passe est changé après toute utilisation par un tiers.

8.4.3. Gestion des comptes système personnels

Les comptes système personnels sont des comptes privilégiés nominatifs avec des privilèges / droits équivalents aux comptes système qu'ils remplacent.

Des comptes systèmes nominatifs sont créés pour chaque personne justifiant de l'utilisation d'un compte privilégié. Ils diffèrent des comptes « bureautiques » ou « applicatifs » de leurs titulaires.

8.4.4. Gestion des comptes système utilisés par les constructeurs

Il s'agit principalement de comptes destinés à l'installation ou à la maintenance des matériels et des logiciels.

Les comptes destinés uniquement à l'installation des produits sont supprimés, ou au minimum désactivé, dès l'installation terminée.

Les comptes destinés uniquement à la maintenance sont désactivés en dehors des opérations de maintenance ou leurs mots de passe changés dès la fin de toute opération de maintenance.

8.4.5. Authentification des comptes à privilèges élevés

Les mots de passe sont modifiés

- Après expiration du mot de passe (temps de vie expiré)
- Après toute intervention de maintenance ou utilisation temporaire du compte par un tiers (ex : compte de production utilisé ponctuellement par un développeur).
- Dès qu'une personne sort de la liste des utilisateurs autorisés.

8.4.6. Disponibilité des comptes à privilèges élevés

Des mesures permettent d'assurer la disponibilité des mots de passe des comptes privilégiés (mise sous enveloppe et conservation dans un lieu sécurisé).

8.4.7. Restriction d'emploi des utilitaires systèmes et de sécurité

L'utilisation des programmes permettant de contourner les mesures de sécurité, notamment en accédant directement à l'information stockée ou transportée, sans passer par la couche applicative, est fortement encadrée et tracée, et réservée aux administrateurs autorisés. Il en va de même pour l'utilisation de tout utilitaire de sécurité, permettant par exemple de connaître ou de manipuler le paramétrage des systèmes, d'accéder aux fichiers de journalisation, ou de réaliser toute autre action dangereuse.

L'installation et l'utilisation de tels outils par des utilisateurs non administrateurs est obligatoirement justifiée et préalablement autorisée par le RSSI.

8.5. Séparation des rôles

8.5.1. Séparation des tâches

Afin de limiter les risques d'erreur ou de mauvais usage, il convient d'établir une séparation des tâches et des responsabilités entre ;

Au niveau fonctionnel :

- Les administrateurs systèmes et réseaux
- Les administrateurs bases de données

Au niveau système :

- Les personnes chargées de l'exploitation des infrastructures support du SI
- Et les personnes chargées d'en contrôler l'utilisation

Au niveau des comptes applicatifs :

- Les personnes chargées d'autoriser les droits d'accès applicatifs.
- Les personnes utilisant les comptes applicatifs.
- Et les personnes chargées d'attribuer les droits.

8.5.2. Séparation des environnements

Les différents environnements et équipements (développement, test, exploitation…) sont séparés.

Les règles de passage d'un environnement à l'autre sont formalisées et documentées.

Il serait souhaitable que les données opérationnelles soient « blanchies » s'il est nécessaire de les utiliser pour des besoins de développement ou de test.

9. Sécurité des réseaux

9.1. Architecture des réseaux

9.1.1. Passerelles Internet et de sécurité

Des équipements d'infrastructure sont mis en place afin de protéger et d'isoler les réseaux internes vis-à-vis de l'extérieur.

Cette utilisation de passerelles a pour but de faciliter la gestion de la sécurité réseau tout en limitant les risques qui proviendraient de la multiplicité et de la variété des moyens d'échange et d'accès.

9.1.2. Plan d'adressage

Des adresses IP non routables et un mécanisme de traduction d'adresses sont utilisés afin de protéger en confidentialité le plan d'adressage interne vis-à-vis de l'extérieur.

Le plan d'adressage est diffusé aux seuls ayant droits.

9.1.3. Maillage des liaisons

Tout service réseau est analysé d'un point de vue disponibilité afin d'évaluer sa criticité vis-à-vis des besoins de l'Université de Tours et des utilisateurs, et dimensionné en conséquence.

9.1.4. Cloisonnement des réseaux

Des zones ou périmètres de sécurité sont définies afin de cloisonner le système d'information en périmètres de niveaux de confiance homogènes différents :

- *Réseau Internet* : zones directement connectées à Internet, non maîtrisées et disposant d'un niveau de confiance nul.
- *LAN Internet* : zones de confiance basse, ouvertes sur le réseau Internet au travers d'une DMZ.
- *LAN interne* : zones maîtrisées disposant d'un bon niveau de confiance. Elles hébergent l'ensemble des ressources du système d'information. Ces zones n'ont pas de connexion avec le réseau Internet.
- *DMZ* : zones maîtrisées mais disposant d'un niveau de confiance modéré. Elles hébergent les équipements assurant l'interface entre les LAN internes d'une part, le réseau Internet d'autre part, et garantissent la protection des premiers vis-à-vis du second.

Aucun équipement de l'Université de Tours ne peut être connecté directement au Réseau Internet. Toute connexion transite par une DMZ. Toute exception fait l'objet d'une demande de dérogation.

9.1.5. Partitionnement des réseaux

Le LAN interne est partitionné en sous-réseaux afin d'assurer un isolement des « branches sensibles » et de permettre de confiner, si besoin est, une branche réseau en cas d'incident.

Les connexions sont filtrées et un contrôle d'accès activé au niveau d'un sous-réseau.

Un cloisonnement à minima est réalisé pour séparer les périmètres suivants :

- Les serveurs dans un réseau avec des protections adaptées
- Les postes administratifs
- Les postes d'enseignement
- Les postes de recherche
- Les postes d'étudiants
- Les laboratoires de recherche
- Les communications en wifi
- L'administration des équipements
- La téléphonie

9.1.6. Isolement des réseaux sensibles

Sont considérés comme réseaux sensibles :

- Les réseaux hébergeant des serveurs ou applications contenant des informations sensibles ou des processus métier sensibles, tels que les serveurs d'applications en production, les serveurs de sécurité (annuaire, firewall, proxy, serveur d'authentification), les serveurs de sauvegarde, les réseaux des laboratoires, les réseaux de téléphonie, les réseaux de développement.
- Les réseaux pour lesquels la sécurité n'est pas connue ou maîtrisée par l'Université de Tours (réseaux d'un partenaire, d'un laboratoire).

Il convient de cloisonner les réseaux sensibles vis-à-vis du LAN interne par des mesures de sécurité réseau (pare-feu, antivirus, proxy, VLAN, authentification...).

Tout accès depuis un réseau extérieur sur une machine connectée à un réseau de l'Université de Tours est soumis à autorisation et validé de manière formelle en cohérence avec la politique d'accès de l'Université de Tours.

9.2. Documentation des réseaux

9.2.1. Identification de l'infrastructure réseau

L'infrastructure réseau est répertoriée et documentée. Il existe une description à jour de cette infrastructure incluant :

- Une cartographie du réseau recensant les principaux éléments de l'infrastructure et présentant l'organisation générale du réseau (Ligne Spécialisée, LAN, accès Internet, autre accès...),

- Un dossier de sécurité réseau, définissant l'infrastructure réseau (interface sur l'extérieur, équipements réseaux, etc.),
- Un recensement des principaux flux de données internes ou externes,
- Un descriptif détaillé du câblage interne,
- Un inventaire des équipements, leur localisation et leur configuration,
- Une description des moyens de sécurisation utilisés (filtrage, chiffrement, authentification, ...) et de leur mise en œuvre opérationnelle au niveau des équipements de sécurité réseau.

La documentation réseau est actualisée lors de toute modification fonctionnelle des flux ou de l'infrastructure technique du réseau.

Elle est revue au minimum une fois par an.

9.2.2. Documentation d'administration et d'exploitation des réseaux

Les procédures d'exploitation du réseau sont formalisées et documentées. Parmi ces procédures, une attention toute particulière est apportée à la procédure d'ouverture de règles au niveau des équipements de filtrage réseau.

Les éléments (documents, fichiers) décrivant l'infrastructure réseau et sa configuration sont documentés.

La documentation est tenue à jour. L'accès à cette documentation est limité aux personnes disposant du besoin d'en connaître.

9.2.3. Protection de la documentation et des données réseau

La documentation réseau et les procédures d'administration et d'exploitation des réseaux sont des documents sensibles ; elles sont protégées contre tout accès non autorisé par des personnes ne disposant pas du besoin d'en connaître.

Des mesures mise en œuvre par la DSI garantissent la disponibilité et l'intégrité de ces éléments.

9.3. Administration et exploitation des réseaux

9.3.1. Journaux des opérations d'administration et d'exploitation des réseaux

Les opérations sensibles d'administration sont tracées et journalisées, via l'enregistrement des connexions et modifications effectuées.

Les journaux sont sauvegardés et conservés pendant une période adaptée aux besoins de suivi et contrôle, en respectant les exigences réglementaires.

9.3.2. Dimensionnement des réseaux

Il convient de surveiller les activités réseaux et de s'assurer que l'infrastructure réponde aux besoins de disponibilité, de dimensionnement et de qualité de service de l'Université de Tours.

9.3.3. Contrôle d'accès logique aux équipements réseau

Un contrôle d'accès logique aux équipements réseaux est mis en œuvre.

Les mots de passe constructeur par défaut sur les équipements sont systématiquement désactivés. Si possible, des comptes d'administration et de supervision nominatifs sont créés. Les mots de passe sont régulièrement modifiés.

Il est régulièrement procédé à un contrôle des accès aux équipements réseau et des droits alloués aux administrateurs et aux exploitants.

9.3.4. Protection de l'administration réseau

L'administration et la supervision des réseaux sont effectuées depuis des réseaux et des équipements dédiés.

L'accès aux ports (physiques et logiques) d'administration et de supervision est contrôlé et limité aux équipements ou réseaux dédiés.

9.3.5. Surveillance continue de l'activité sur les réseaux

La DSI assure une surveillance continue des réseaux sous sa responsabilité.

Cette surveillance porte notamment sur :

- Le contrôle du bon fonctionnement des réseaux.
- Le contrôle de la charge des réseaux et de leur disponibilité.
- L'utilisation réalisée au travers des réseaux.

Cette surveillance s'appuie sur des moyens dédiés et protégés, qui sont éventuellement partagés avec ceux utilisés pour l'administration et l'exploitation des systèmes et des réseaux.

9.3.6. Journalisation des événements réseau

Des dispositifs d'audit sont mis en place qui permettent l'enregistrement dans des fichiers de traces (dits journaux d'audit) des principaux événements liés à la sécurité des réseaux.

Cette journalisation porte notamment sur les événements suivants :

- Les anomalies pouvant être révélatrices d'un incident de sécurité.
- Les atteintes à la sécurité : détections de virus, tentatives d'intrusion, erreurs de connexion, etc.

- L'activité des personnes en charge de l'exploitation des réseaux : configuration et paramétrage des équipements de communication, gestion des habilitations et des droits d'accès, etc.
- Les événements liés à : accès réseau, sites consultés, volumétrie des échanges, connexions des nomades, etc.

Les journaux d'audit sont systématiquement revus afin de détecter les problèmes de sécurité. Les événements révélateurs d'un possible problème de sécurité sont analysés quotidiennement. Les autres événements (traces d'activités de gestion ou d'utilisation des SI par exemple) sont revus sur une base hebdomadaire.

9.3.7. Conservation des journaux réseau

Les journaux d'audit sont des biens sensibles, qui sont sauvegardés et protégés. Ils sont conservés pendant une période suffisante pour répondre aux besoins opérationnels tout en satisfaisant les exigences légales, réglementaires ou contractuelles.

9.4. Sécurité de l'infrastructure réseau

Par infrastructure réseau, on entend les équipements matériels et logiciels, le câblage, les prises réseaux.

9.4.1. Sécurisation des équipements d'infrastructure réseau

Les configurations des équipements d'infrastructure réseau bénéficient de mesures de durcissement

Des procédures de durcissement sont définies et appliquées. Elles concernent a minima les aspects :

- Sécurisation de l'accès, contrôle d'accès logique à l'interface d'administration
- Sélection des composants logiciels, désactivation des utilitaires et paquetages non utilisés
- Gestion des comptes et privilèges d'administration
- Mises à jour des correctifs de sécurité
- Activation des traces d'audit
- Stratégie de sécurité (mot de passe, verrouillage)

9.4.2. Protection du câblage et des prises réseau

Les prises réseau sont identifiées et localisées, et seules les prises utilisées sont brassées. L'accès aux panneaux de raccordement et aux tableaux de brassage est contrôlé. L'accès aux têtes de ligne est contrôlé et protégé. Les câbles de l'infrastructure réseau sont protégés contre les risques d'interception ou de dommage.

9.4.3. Disponibilité des équipements réseau

Les équipements d'infrastructure critiques (tels que les routeurs, les commutateurs fédérateurs) sont dupliqués ; à défaut, des matériels de remplacement sont disponibles.

9.5. Équipements non maîtrisés par l'Université de Tours

Par équipements non maîtrisés par l'Université de Tours, on entend les équipements réseau (modems, routeurs, etc.) voire de sécurité (ces équipements peuvent contenir des fonctions de sécurité) mis en œuvre ou administrés par des tiers (Ces tiers sont généralement des opérateurs de télécommunication. Ces équipements peuvent être la propriété de l'Université de Tours ou de ces tiers. Leur installation peut être faite sous la responsabilité de l'Université de Tours ou de ces tiers.

9.5.1. Identification des équipements non maîtrisés

Il convient d'identifier et répertorier les équipements réseau et de sécurité non maîtrisés par l'Université de Tours. Leur utilisation fait l'objet d'une étude de sécurité et d'une autorisation préalable à leur installation.

9.5.2. Protection de sécurité des équipements non maîtrisés

En l'absence d'un contrat spécifique prenant en compte la sécurité, il convient de considérer comme inexistantes les fonctions de sécurité disponibles sur les équipements non maîtrisés par l'Université de Tours.

Les mesures de sécurité ne doivent pas reposer sur celles proposées par les équipements non maîtrisés, tels que fournis par les services des Fournisseurs d'Accès Internet (sauf contractualisation spécifique).

Il convient de doubler tout équipement non maîtrisé par l'Université de Tours pouvant avoir un impact potentiel négatif pour la sécurité, par un équipement réseau ou de sécurité permettant de contrer les risques identifiés.

10. Sécurité des échanges de données

10.1. Dispositions générales sur les flux réseaux

10.1.1. Contrôle des accès réseau

L'accès à Internet donne lieu à journalisation des accès.

Un mécanisme d'authentification renforcée est utilisé pour les accès entrants depuis un Réseau Internet vers le LAN internet.

10.1.2. Protection des flux réseau

Tout échange entre l'Université de Tours et l'extérieur respecte le principe du moindre privilège.

Les règles relatives aux flux d'informations sont :

- Tout flux d'information établi entre l'Université de Tours et un réseau dit « non sûr » transite obligatoirement par une plate-forme d'interconnexion.
- Les flux échangés entre l'Université de Tours et l'extérieur sont journalisés.
- Tout flux d'un niveau de sensibilité donné est protégé (chiffrement, scellement, signature) lorsque cela est nécessaire.

10.1.3. Analyse des flux réseau

Tous les flux réseaux entrants sont analysés par un mécanisme de détection d'intrusion.

Tous les mails sont analysés par un système d'antispam et d'antivirus.

Les flux jugés dangereux (mails, attaques, etc.) sont détruits.

10.1.4. Traçabilité, surveillance et alerte

Des équipements sont mis en œuvre pour assurer la traçabilité des accès et des flux entrants et sortants avec le réseau Internet, et pour l'accès aux applications métiers sensibles.

Les événements tracés sont enregistrés et les traces protégées en intégrité.

Les équipes réseau effectuent un monitoring des événements critiques (alarmes) remontés par les équipements ainsi qu'une analyse quotidienne des journaux d'événements. Les alarmes et les événements susceptibles de révéler un incident de sécurité sont investigués.

10.1.5. Utilisation de la voix sur IP

Une politique relative à l'utilisation éventuelle des systèmes de communication sur IP, et des applications type "Skype" est définie et appliquée.

10.2. Accès à l'Internet depuis le réseau interne de l'Université de Tours

Ces accès sont caractérisés par le fait que les sites et services accédés ont un niveau de confiance inconnu.

10.2.1. Autorisation d'accès à Internet

L'accès au réseau Internet (web) est systématiquement autorisé. Il peut être retiré sur demande de la hiérarchie ou de la DSI en cas de violation des règles d'usage du service.

L'accès alloué est personnel. Il est réservé à un usage professionnel.

Les utilisations de cet accès sont tracées et journalisées et font l'objet d'un examen périodique.

10.2.2. Diffusion des règles d'accès et d'utilisation

Les règles régissant la navigation sur Internet et l'utilisation des outils de communication sont formalisées dans une charte utilisateur, diffusées à l'ensemble du personnel, connues et acceptées. Elles sont notamment rappelées lors des sessions de sensibilisation à la sécurité.

10.2.3. Analyse des fichiers entrants et sortants

Dans la mesure du possible, tout contenu transmis ou récupéré par un utilisateur fait l'objet d'une analyse antivirale, soit par l'antivirus du poste de travail, soit par un antivirus de passerelle, ou encore par une station dédiée. Cela s'applique en particulier outre les fichiers transmis par mail, à tous les fichiers téléchargés.

10.2.4. Contrôle des accès et de l'utilisation

Des mesures de contrôle d'accès et d'utilisation de l'Internet sont mises en œuvre :

- Dans la mesure du possible, les contenus des flux sont analysés à la recherche de virus, codes mobiles ou signatures d'attaque.
- Toutes les connexions sont tracées, journalisées et régulièrement auditées.

10.3. Accès aux sites Web de l'Université de Tours depuis l'Internet

Ces accès sont caractérisés par le fait que le tiers accédant n'est pas, a priori, « de confiance ». Ce peut être par exemple un laboratoire, un partenaire, un étudiant et tous les accès volontairement malveillants.

- Ces sites et services Web permettent :
- La publication d'informations destinées à tous
- Le recueil d'informations issues des tiers identifiées ou non identifiés

10.3.1. Publication de données sur Internet

Les informations destinées à être publiées sont validées préalablement à leur mise en ligne. L'authenticité des informations mises en ligne est régulièrement contrôlée par leur propriétaire.

Il convient que la mise à disposition d'informations particulières telles que programmes, patches ou fichiers de configuration soit toujours associée à celle d'un motif d'intégrité ou d'un scellement permettant à un tiers d'en contrôler l'intégrité.

10.3.2. Recueil d'informations personnelles auprès de tiers (connus ou inconnus)

Ces informations (demandes, coordonnées...) sont collectées par l'Université de Tours dans un but précis et peuvent être confidentielles ou à caractère personnel. À ce titre :

- Les informations collectées sont protégées contre tout accès non autorisé.
- La personne doit être explicitement informée de la finalité du recueil ainsi que de son droit de consultation et de rectification ou suppression des données personnelles recueillies.

10.3.3. Contrôle des informations mises à disposition

Les informations reçues et mises à disposition par l'Université de Tours, sont analysées (recherche de virus et de codes mobiles, détection de signatures d'attaque...) et filtrées afin d'éliminer tout élément malveillant, et d'éviter sa retransmission.

10.3.4. Protection des mécanismes de recueil d'information via le web

Les mécanismes de recueil sont protégés contre les attaques par une rupture des flux entre Internet et le système d'information (utilisation d'un serveur mandataire).

10.4. Accès pour les partenaires et accès à des services tiers externes

Ces échanges sont établis avec des partenaires connus et identifiés et répondent à des besoins « formalisables ». Ils permettent :

- La mise à disposition avec ces partenaires d'informations à diffusion limitée
- L'utilisation, depuis l'Internet ou le LAN Interne, d'applicatifs permettant de gérer des données qualifiées

Des échanges spécifiques, (tel que la transmission d'ordres de virement). Ces échanges s'appuient souvent sur des protocoles spécialisés et des outils dédiés.

10.4.1. Formalisation des services et des échanges applicatifs

Les services et les échanges applicatifs mis à la disposition de tiers comme l'utilisation de services tiers externes sont définis dans le cadre de projets qui incluent une analyse sécurité permettant :

- D'identifier les connexions et flux de données nécessaires sur un plan fonctionnel ou technique.

- De déterminer leurs besoins de sécurité (confidentialité, intégrité, authenticité, non-répudiation).
- D'évaluer la menace et les risques induits.
- De sélectionner des contre-mesures permettant de ramener ces risques à un niveau acceptable.

10.4.2. Autorisation d'accès

L'ouverture d'un accès pour un tiers est soumise à autorisation et nécessite la signature d'un accord préalable entre ce tiers et l'Université de Tours. Il en est de même pour tout accès à un service tiers externe. Ces accords contractuels incluent l'aspect sécurité et définissent les procédures à respecter.

10.4.3. Contrôle des accès et protection des échanges

Le tiers – système, applicatif ou utilisateur – accédant au système d'information de l'Université de Tours, est identifié et authentifié. L'utilisation d'un protocole sécurisé (SSL, SSH) ou d'une liaison garantissant cette identité (LS, VPN) est recommandée.

L'autorisation et les moyens cryptographiques utilisés sont soumis à validation par le Comité de Sécurité Opérationnelle.

Des mesures de sécurité spécifiques sont mises en œuvre en fonction de la sensibilité des informations échangées (chiffrement, scellement, signature...).

Les connexions établies et les échanges réalisés sont tracés, journalisés et régulièrement audités.

10.5. Utilisation du Wifi

10.5.1. Utilisation du Wifi dans l'Université de Tours

L'accès aux points de connexion Wifi est contrôlé, et réservé aux seuls utilisateurs autorisés.

Des mesures d'authentification des utilisateurs accédant aux points d'accès Wifi, et des mesures de chiffrement des flux Wifi sont réalisées en fonction du besoin. Les conditions d'usage des réseaux

Wifi et la responsabilité des utilisateurs y accédant sont formalisées dans une charte utilisateur. La charte est diffusée aux utilisateurs préalablement à leur utilisation du Wifi.

11. Sécurité des serveurs et des systèmes

Par systèmes et serveurs, on entend les serveurs bureautiques, les serveurs applicatifs et les serveurs dits d'infrastructure (serveurs hébergeant des services transversaux nécessaires au fonctionnement du SI : serveurs de messagerie, serveurs de domaine Active Directory), ainsi que les systèmes dits de sécurité tels que des pare-feu, serveurs antivirus, proxys, etc.

11.1. Configuration et gestion des configurations

11.1.1. Sécurisation des serveurs

Les systèmes d'exploitation des serveurs bénéficient de mesures de durcissement concernent à minima :

- Sécurisation de l'accès au BIOS, contrôle d'accès logique au système
- Désactivation des ports et services non utilisés (Telnet, rlogin, ftp, etc...)
- Sélection des composants logiciels, désactivation des utilitaires et paquetages non utilisés
- Gestion des comptes et privilèges d'administration
- Mises à jour des correctifs de sécurité
- Activation des traces d'audit
- Stratégie de sécurité (mot de passe, verrouillage)

11.1.2. Documentation des procédures d'exploitation

Les procédures d'exploitation des systèmes informatiques sont documentées.

Cette documentation précise les instructions à suivre pour toute tâche qui relève de l'administration, de l'exploitation, de la supervision et de la maintenance des systèmes informatiques. Elle est tenue à jour, actualisée si nécessaire, et revue au minimum une fois par an.

Seules les personnes ayant le besoin d'en connaître accèdent à cette documentation.

11.1.3. Maîtrise des modifications et des configurations

Les configurations des systèmes informatiques et les modifications de ces systèmes font l'objet d'un contrôle strict. Une procédure précise les conditions de mise en œuvre des modifications.

Les impacts des modifications sont évalués et les changements testés.

Les modifications importantes sont planifiées. Il convient de définir une procédure de repli.

Les configurations des SI sont documentées. Tous les changements sont consignés.

11.2. Administration des serveurs et des systèmes

11.2.1. Installation et hébergement

Les serveurs sont installés dans des locaux dédiés, sécurisés (contrôle d'accès, protection environnementale, télésurveillance) adaptés à la sensibilité des données qu'ils traitent et des informations qu'ils hébergent.

11.2.2. Systèmes a priori sensibles

Les systèmes suivants sont automatiquement considérés comme sensibles et sont protégés :

- Contrôleurs de domaine
- Serveurs antivirus
- Serveurs de messagerie
- Serveurs Web, serveurs FTP et autres serveurs d'échanges
- Serveurs applicatifs
- Serveurs de journaux
- Serveurs de noms DNS

11.2.3. Disponibilité des serveurs sensibles

Les serveurs d'infrastructure sont systématiquement redondés.

Il convient d'estimer la nécessité d'une redondance, de dispositif de secours ou de contrat de maintenance adapté pour les serveurs bureautiques ou applicatifs en fonction des besoins de disponibilité analysés.

11.2.4. Administration et supervision

L'administration et la supervision des serveurs sont réalisées par des personnels autorisés depuis des environnements protégés (locaux, VLAN, consoles de supervision).

Les flux d'administration et de supervision sont protégés en confidentialité.

Les actions d'administration et de supervision sont tracées et font l'objet de revues si besoin.

11.2.5. Déconnexion automatique des sessions

Une période d'inactivité des sessions d'administration est définie pour les systèmes sensibles, au-delà de laquelle une nouvelle identification et authentification sont rendues obligatoires.

11.2.6. Synchronisation des horloges

Les ressources informatiques nécessitant de disposer d'un horaire fiable pour leurs traitements ou pour la production de log d'enregistrement, sont synchronisées à un système de référence de temps.

11.3. Systèmes d'impression

11.3.1. Protection de l'administration par mot de passe des imprimantes

Les fonctions d'administration locales ou distantes des imprimantes mutualisées qui reçoivent des données sensibles, sont protégées par mot de passe.

11.3.2. Configuration des imprimantes

Les données mémorisées sur les imprimantes mutualisées sont régulièrement effacées par les administrateurs.

Les imprimantes mutualisées sont configurées afin de ne pas pouvoir transmettre directement des documents scannés par mail à l'extérieur de l'établissement.

11.3.3. Protection des impressions

Des mesures organisationnelles permettent de limiter le temps de présence des impressions sensibles sur les imprimantes.

Les impressions sensibles sont réalisées sur des imprimantes contrôlées (localisation physique protégée, imprimantes sur un réseau contrôlé), et configurées pour permettre au seul propriétaire de pouvoir récupérer les impressions.

11.4. Surveillance et journalisation

11.4.1. Surveillance continue des systèmes

La DSI assure une surveillance continue des systèmes et serveurs sous sa responsabilité.

Cette surveillance porte notamment sur :

- Le contrôle du bon fonctionnement du système d'information.
- Le contrôle de la charge des systèmes et serveurs et de leur disponibilité.
- L'utilisation des systèmes d'information et des serveurs.

Cette surveillance s'appuie sur des moyens dédiés et protégés, qui sont éventuellement partagés avec ceux utilisés pour l'administration et l'exploitation des systèmes et des réseaux.

11.4.2. Journalisation des événements système

Les principaux événements liés à la sécurité sont enregistrés dans des fichiers de traces.

Cette journalisation porte notamment sur les événements suivants :

- Les anomalies pouvant être révélatrices d'un incident de sécurité.
- Les atteintes à la sécurité : détections de virus, tentatives d'intrusion, erreurs de connexion...

- L'activité des personnes en charge de l'exploitation du SI : configuration et paramétrage des systèmes, gestion des habilitations et des droits d'accès...
- L'activité « système » des utilisateurs : connexions et déconnexions, accès et utilisation des ressources sensibles du système d'information...

Il convient de réexaminer périodiquement les résultats des activités de surveillance.

11.4.3. Conformité des dispositifs de surveillance et de journalisation

Il convient de s'assurer que les dispositifs de surveillance et de journalisation mis en œuvre sont conformes à la législation en vigueur, adaptés et proportionnels à l'enjeu et aux risques encourus : il convient de s'assurer que les informations journalisées respectent les exigences légales et réglementaires en matière de trace ainsi que la vie privée des utilisateurs (données personnelles).

Il convient notamment d'informer les instances représentatives des personnels lors du choix de ces dispositifs et de la définition des modalités d'utilisation, et d'informer les utilisateurs de leur mise en œuvre.

11.4.4. Conservation des journaux systèmes

Les journaux d'audit sont des biens sensibles, qui doivent être sauvegardés et protégés. Ils sont conservés pendant une période suffisante pour répondre aux besoins opérationnels et satisfaire les exigences légales, réglementaires ou contractuelles.

12. Sécurité des applications et des données applicatives

12.1. Administration des applications

12.1.1. Gestion des autorisations d'accès aux applications

Les autorisations d'accès aux applications (attribution d'un droit d'accès, révision, retrait) s'appuient sur des règles et procédures mises en place au titre du processus de gestion des habilitations et des droits d'accès.

Les droits alloués sont régulièrement réévalués.

12.1.2. Contrôle d'accès aux applications

L'accès aux applications est contrôlé. Ce contrôle d'accès s'appuie sur les mécanismes mis en œuvre au titre de l'identification des utilisateurs, de leur authentification et des droits hérités de leur profil et du contexte d'utilisation.

Ces mécanismes conditionnent également l'accès aux différentes fonctions et données au sein des applications.

L'accès alloué à un utilisateur est strictement personnel.

12.1.3. Contrôle et suivi de l'utilisation des applications

Les utilisations des fonctions applicatives sont tracées et journalisées (en fonction de leur sensibilité et des données accédées).

Les journaux applicatifs sont régulièrement analysés afin de détecter les erreurs d'utilisation, les dysfonctionnements et les utilisations illicites.

12.2. Sécurité des applications

12.2.1. Validation des données et fonctions applicatives

Une vérification des données transmises aux applications sensibles est effectuée afin d'empêcher des conditions pouvant porter atteinte à la sécurité des fonctions ou des informations des applications (valeurs hors intervalle, caractères invalides, données incomplètes, etc.)

La conception et la mise en œuvre des applications doivent réduire les risques de pertes d'intégrité. Les droits de lecture, écriture, exécution sont ajustés au besoin.

En fonction de leur sensibilité, les applications alimentées en sources externes de données contrôlent l'intégrité des messages et données reçues.

Les tests de recettes des applications sont réalisés de manière systématique afin de s'assurer que les bonnes pratiques de sécurité ont été prises en compte.

12.2.2. Limitation de durée de connexion

Les applications sensibles mettent en œuvre des limitations du temps de connexion, par tranche horaire, par durée de connexion, ou par durée d'inactivité. Les utilisateurs doivent alors se ré-authentifier pour continuer l'usage de ces applications sensibles.

12.3. Utilisation de la cryptographie

12.3.1. Éléments cryptographiques

La gestion des clés secrètes ou des bi clés utilisées en support de mécanismes d'authentification, de chiffrement ou de signature est adaptée à la sensibilité des données traitées et à la nature des échanges mis en œuvre. Toute utilisation d'éléments cryptographiques est sujette à demande préalable auprès du comité de sécurité opérationnelle, qui s'assurera en particulier de la recevabilité des principes de gestion envisagés au regard des exigences règlementaires.

12.3.2. Algorithmes et outils cryptologiques

Une liste des algorithmes autorisés et des outils recommandés est définie et gérée par le Comité de Sécurité Opérationnelle. Les solutions retenues pour mettre en place des mécanismes de chiffrement, d'authentification ou de signature doivent être choisies dans cette liste. L'utilisation est agréée par le RSSI qui peut autoriser des dérogations en cas d'inadéquation des solutions référencées.

13. Sécurité de l'environnement utilisateur

13.1. Poste de travail

13.1.1. Attribution des postes de travail

L'attribution d'un poste de travail est soumise à autorisation par le responsable hiérarchique ; les usagers autorisés s'engagent à respecter les règles d'usage afférentes au poste.

13.1.2. Identification des postes de travail

Tout poste appartenant à l'université de Tours est inventorié. Il existe un inventaire de l'ensemble des postes de travail, de leur localisation « principale », de leur spécificité, et de leur utilisateur.

13.1.3. Rappel des règles de protection des postes de travail

Les principales règles et dispositions relatives à la sécurité des postes de travail et à leur utilisation sont rappelées dans une charte utilisateur disponibles sur l'intranet.

Les utilisateurs sont sensibilisés à l'usage de moyens de protection physique des postes et matériels de travail en dehors de leur présence (fermeture des locaux, rangements dans des armoires fermées à clé, etc.)

13.1.4. Administration des postes de travail

En règle générale, l'utilisateur ne dispose pas des droits lui permettant de réaliser des opérations d'administration sur son poste de travail.

L'administration d'un poste de travail bureautique par son utilisateur reste une exception. Elle fait l'objet d'une demande formelle motivée et validée par la hiérarchie de l'utilisateur.

13.1.5. Sécurité des postes de travail

Des mesures de sécurité sur les postes de travail concernent à minima :

- Les conditions d'accès (identification et authentification obligatoire),
- L'intégrité du poste (outils anti-virus, pas de droit d'administration),
- La disponibilité des informations (processus de sauvegarde locale ou distante).

Sauf cas exceptionnel, l'utilisateur ne conserve pas de données sensibles sur son poste de travail mais uniquement sur les serveurs de fichiers.

Dans le cas où l'utilisateur conserve des données sensibles sur son poste de travail, celles-ci devront être placées dans un répertoire sécurisé, garantissant la confidentialité, la disponibilité, l'intégrité et la traçabilité.

13.2. Supports informatiques mobiles

13.2.1. Usage des supports d'informations amovibles et mobiles.

Il convient de mettre en place des procédures pour la gestion des supports amovibles.

13.2.2. Stockage d'une information sensible sur support amovible ou mobile

Dès lors qu'elles sont stockées sur un support amovible ou mobile, les informations sensibles font l'objet d'un chiffrement approprié.

13.2.3. Politique du bureau propre

Les personnels de l'Université de Tours ne laissent pas d'informations sensibles exposées à la vue ou à la convoitise de personnes non autorisées ; en particulier, chaque personne est responsable du rangement de son bureau ou des espaces partagés qu'elle utilise.

Les supports (tableaux, paperboards, papiers, ...) utilisés dans des locaux partagés pour traiter des informations sensibles sont systématiquement effacés ou détruits.

13.2.4. Mise au rebut des supports amovibles

Les supports de données mobiles ou amovibles (disque dur, DVD, papier, etc.) contenant de l'information sensible sont préalablement effacés avant leur mise au rebut.

13.3. Bureautique

13.3.1. Sécurité des documents bureautiques utilisateurs

Des espaces bureautiques sécurisés et sauvegardés sont mis à la disposition de chaque utilisateur. L'accès à ces espaces utilisateurs sécurisés est limité à l'utilisateur et aux administrateurs autorisés.

Les documents bureautiques confidentiels sont stockés dans ces espaces sécurisés et sauvegardés.

13.3.2. Sécurité des espaces bureautiques partagés

Des espaces bureautiques partagés sécurisés et sauvegardés sont créés à la demande (pour des projets, des applications bureautiques).

L'accès à ces espaces partagés est sous le contrôle d'un responsable identifié.

Les documents bureautiques confidentiels partagés sont stockés dans ces espaces partagés sécurisés et sauvegardés.

13.4. Messagerie

13.4.1. Formalisation des règles d'utilisation de la messagerie électronique

Les règles relatives à l'utilisation de la messagerie sont rappelées dans la charte utilisateur.

13.4.2. Contrôle d'accès à la messagerie électronique

L'accès à la messagerie nécessite une identification et authentification préalable de l'utilisateur.

13.4.3. Analyse des messages

Les messages électroniques sont systématiquement analysés par un antivirus d'une technologie différente de celle employée sur les postes de travail.

13.4.4. Chiffrement et contrôle d'intégrité des messages et pièces jointes

Il convient de protéger de manière adéquate les informations transitant par la messagerie électronique.

14. Mobilité

14.1. Sécurité des postes nomades

14.1.1. Politique de sécurité des nomades

La politique de sécurité des postes nomades est rappelée dans la charte d'usage et traite à minima les points suivants :

- Ouverture de session protégée par mot de passe
- Obligation d'un mode d'accès sécurisé (VPN) pour l'accès au réseau interne
- Utilisation de moyens de chiffrement des données sur les postes nomades,
- Rappel des risques de connexions sur des moyens non sûr avec ses identifiants universitaires (cybercafé, borne, ...)

14.1.2. Attribution d'un accès nomade

L'attribution d'un accès nomade est soumise à autorisation par le responsable hiérarchique ; les usagers autorisés s'engagent à respecter les règles d'usages des moyens d'accès nomades.

14.1.3. Connexions des postes nomades

Les accès distants d'un poste nomade au système d'information de l'Université de Tours mettent en œuvre un mécanisme d'authentification renforcée.

14.2. Utilisation de matériel hors des locaux

14.2.1. Dispositifs de sécurité installés sur les nomades

Tout poste nomade comprend par défaut :

- Un antivirus.
- Un logiciel de chiffrement de disque et/ou des fichiers.

Selon les besoins identifiés et les informations traitées, des configurations durcies peuvent être mises à disposition des usagers : authentification forte pour la connexion au poste, outil de sécurisation de la connexion VPN, outil de chiffrement des disques durs, support amovible sécurisé, outil de contrôle de double connexion.

14.2.2. Utilisation des postes nomades à l'extérieur

La politique d'usage des postes nomades à l'extérieur est rappelée dans la charte d'usage. Elle traite à minima les points suivants :

- Les conditions d'utilisation du poste (restrictions, surveillance, stockage...).
- Les règles spécifiques destinées à assurer la sécurité des données stockées ou traitées.

- Les règles relatives à des problématiques particulières (démonstration, passage en douane, pays à risque...).

14.2.3. Mises à jour et correctifs de sécurité des postes nomades

Des moyens sont mis en place afin de s'assurer que les mises à jour et correctifs de sécurité des postes nomades sont systématiquement exécutés avant leur reconnexion au réseau interne de l'Université de Tours.

Les moyens mis en place s'assurent de l'authenticité des mises à jour et correctifs reçus ou téléchargés.

Leur intégrité est systématiquement contrôlée.

14.3. Télétravail

14.3.1. Télétravail

Il convient d'élaborer et de mettre en œuvre une politique, des procédures et des programmes opérationnels spécifiques au télétravail.

15. Antivirus et code mobile

15.1. Codes malveillants

15.1.1. Existence d'une politique antivirale

La DSI de l'Université de Tours met en œuvre une politique antivirale permettant de protéger les systèmes contre les virus et de gérer et circonscrire les attaques virales.

15.1.2. Disponibilité et utilisation quotidienne des antivirus

La DSI s'assure que tout équipement concerné dispose d'un antivirus actif et à jour et qu'un scan a lieu régulièrement. Cela peut être réalisé par un monitoring permanent ou au minimum par un contrôle périodique systématique.

L'antivirus installé sur le poste de travail effectue régulièrement un scan de l'ensemble des disques locaux afin de s'assurer de l'absence de virus sur le poste.

15.1.3. Détection et traitement des virus

Tout virus détecté déclenche automatiquement une information des équipes concernées de la DSI, par alerte de surveillance et par enregistrement dans les journaux. Ces journaux doivent être examinés périodiquement.

15.2. Code mobile

15.2.1. Détection et traitement des codes mobiles

Il convient que la configuration garantisse que le code mobile fonctionne selon une politique de sécurité clairement définie et il convient d'empêcher tout code mobile non autorisé de s'exécuter.

16. Projet, développement et maintenance

16.1. Sécurité dans les projets du SI

La sécurité est prise en compte à toutes les étapes du cycle de vie d'un projet, interne ou externe, lié au système d'information. Les applications informatiques sont sécurisées, en cohérence avec la sensibilité des informations traitées et échangées.

16.1.1. Analyse et spécifications

Étude et dossier de sécurité

Une identification préalable des projets sensibles (manipulant des données sensibles ou des données personnelles, soumis à des contraintes réglementaires, ou présentant de forts besoins de disponibilité) est réalisée pour identifier les enjeux et les risques.

Tout nouveau projet sensible, ou tout projet ayant de fortes interactions avec le système d'information existant, est précédé d'une étude de sécurité permettant de formaliser les exigences de sécurité à mettre en œuvre. Le Comité de Sécurité Opérationnelle valide les résultats de l'étude.

Formalisation et documentation

L'analyse de sécurité s'appuie sur une méthode et un processus formalisés et documentés. Elle est reprise dans un dossier de sécurité qui accompagne le projet sensible et sera complété au fur et à mesure de l'avancement de celui-ci.

Acquisition de solutions et externalisation des développements

Les cahiers des charges rédigés pour l'acquisition d'une solution sensible (produit, système ou service) ou son développement tiennent compte de l'analyse de sécurité et incluent des clauses qui formulent les exigences et les conditions d'emploi prévues.

Ces cahiers des charges doivent inclure aussi des clauses destinées à assurer la pérennité de ces solutions et prendre en compte la maintenance et les contraintes d'évolution des systèmes et logiciels support dues à la mise en place de correctifs.

16.1.2. Développement

Fonctions et services de sécurité

Les développements doivent respecter des bonnes pratiques, prennent notamment en compte les points suivants :

- L'utilisation de la notion de profil métier pour le contrôle d'accès
- La journalisation des accès et de l'utilisation des différentes fonctions applicatives
- Le contrôle des données d'entrées et des procédures de saisie
- La mise en place de mécanismes de reprise et de gestion des erreurs

- La sécurisation ou le durcissement des équipements, systèmes et configuration
- La mise en œuvre des derniers niveaux de correctifs
- La capacité de sauvegarder et de restaurer les données applicatives

Test et recette des fonctions de sécurité

Les fonctions et services de sécurité retenus et mis en œuvre sont testés et « recettés » avant toute mise en exploitation.

16.1.3. Sécurité du développement et de la maintenance (processus et environnement)

Cloisonnement des environnements

Les environnements de développement et de maintenance, de tests et de pré-production sont distincts de l'environnement exploitation.

Les données utilisées pour le développement et les tests ne sont jamais des données opérationnelles sensibles.

Cloisonnement des rôles

Une séparation marquée des rôles entre tâches de développement, de tests et recette, et d'exploitation est mise en place.

Gestion des sources, des évolutions et des modifications

Les programmes sources, les scripts et les fichiers de paramètres sont gérés en configuration.

L'accès à ces fichiers comme aux données utilisées pour le développement est protégé.

16.2. Suivi d'exploitation

16.2.1. Bon fonctionnement des applications

Les applications sensibles sont hébergées sur des serveurs récents, dont la maintenance « constructeur » est toujours assurée. Il en va de même pour les systèmes d'exploitation.

16.2.2. Politique de journalisation

Une politique de journalisation est mise en place, spécifiant, pour chaque application, les actions à auditer, permettant de collecter, en cas d'attaque ou de dysfonctionnement, les preuves et traces nécessaires au traitement de l'incident. Les délais de rétention des traces sont définis selon la sensibilité des applications.

La politique de journalisation est conforme à la législation en vigueur.

16.3. Maintenance et mises à jour

16.3.1. Gestion et contrôle des opérations de maintenance

Les opérations de maintenance sont documentées (périmètre, actions...) et planifiées en concertation avec les utilisateurs.

Des mesures sont prises (par exemple des tests de non régression) pour vérifier que l'opération de maintenance réalisée n'a pas altéré le système opérationnel.

Un retour en arrière en cas de dysfonctionnement constaté ou d'altération des données faisant suite à l'opération de maintenance réalisée doit toujours être possible.

Les actions de maintenance sont effectuées de préférence localement.

Une présence constante auprès des mainteneurs est assurée pendant que ceux-ci opèrent localement.

Les opérations effectuées au titre des opérations de maintenance sont tracées et journalisées. Un compte-rendu des opérations est systématiquement rédigé.

16.3.2. Télémaintenance

Les services de télémaintenance sont systématiquement encadrés par des accords contractuels qui précisent les conditions dans lesquelles sont effectuées les opérations de télémaintenance.

Les accès de télémaintenance (comptes dédiés, accès réseau) sont fermés en dehors des périodes de télémaintenance. Ils sont ouverts à la demande des télé mainteneurs et à l'initiative des exploitants du système télé maintenu et sont fermés à la fin de toute opération de télémaintenance.

Il convient de s'assurer, via les conditions d'emploi, que les télé mainteneurs informent systématiquement les exploitants de la fin de chaque opération de maintenance afin de leur permettre de fermer les accès.

Les opérations de télémaintenance sont tracées et journalisées. Elles font l'objet d'un contrôle a posteriori systématique.

16.4. Gestion des changements

Par changements, on entend les évolutions du SI traitées par les équipes chargée de l'exploitation.

Ces évolutions concernent principalement l'infrastructure support du SI : évolutions matérielles, évolutions logicielles, mises à jour des configurations...

16.4.1. Mise en œuvre des évolutions logicielles majeures

Les évolutions logicielles majeures sont planifiées. Elles sont testées avant leur mise en œuvre effective.

Une procédure de repli est systématiquement définie.

16.5. Gestion des vulnérabilités techniques et des correctifs

Un processus permet d'être informé en temps voulu de toute vulnérabilité technique relative aux systèmes d'information en exploitation, d'évaluer l'exposition du SI vis-à-vis de ces vulnérabilités et d'entreprendre les actions appropriées pour traiter le risque associé.

16.5.1. Dispositif de veille et d'évaluation des vulnérabilités

Une structure de veille permet d'être informé en temps voulu des vulnérabilités identifiées et des correctifs publiés par les éditeurs ou les sites autorisés (par exemple, les CERT).

La criticité de chaque vulnérabilité (i.e. l'impact qui résulterait de leur exploitation) et de chaque correctif (c'est-à-dire des vulnérabilités corrigées) est évaluée ainsi que les actions à entreprendre. Cette évaluation inclut une détermination du niveau d'urgence de ces actions.

Les corrections de failles de sécurité critiques sur des serveurs sensibles doivent être réalisées au plus tôt.

L'application des autres correctifs de sécurité donne lieu à une analyse évaluant le niveau d'urgence et les impacts des modifications sur la continuité de service.

16.5.2. Gestion des mises à jour et correctifs

Des mesures permettent de s'assurer de l'authenticité des mises à jour et correctifs reçus ou téléchargés. En particulier, ceux concernant les « produits du commerce » sont uniquement obtenus des sites des éditeurs ou de sites sûrs (CERT). Leur intégrité est systématiquement contrôlée.

Dans le cas des systèmes et applications sensibles, les mises à jour et les correctifs sont systématiquement testés et validés préalablement à leur diffusion (i.e. publication sur des serveurs relais internes ou de confiance) ou à leur mise en œuvre dans des environnements de test représentatifs des environnements de production. Ces tests comprennent des tests de compatibilité avec l'existant et des tests de non régression.

Les mises à jour et les correctifs sont appliqués dans des délais cohérents avec leur niveau de criticité et leur niveau d'urgence. Un « plan de gestion des mises à jour et correctifs » définit les règles permettant cette mise en œuvre dans les meilleurs délais, notamment pour les serveurs critiques.

La bonne application des correctifs est contrôlée et mesurée, en particulier sur les postes des utilisateurs, et les mesures nécessaires sont définies pour traiter les systèmes en défaut.

16.6. Fin de vie des projets

16.6.1. Mise au rebut et recyclage en fin de projet

Des moyens techniques sont mis à disposition des administrateurs pour assurer :

- Une destruction sécurisée des documents relatifs au projet.
- - Un effacement sécurisé ou une destruction physique des disques durs et des supports informatiques ayant contenu des données sensibles.

La destruction peut être réalisée par effacement, broyage, ou par enlèvement par une société spécialisée.

16.6.2. Réaffectation des matériels en fin de projet

Préalablement au recyclage, à l'attribution à un nouveau propriétaire ou à la réaffectation d'un poste de travail ou d'un équipement matériel, les informations sensibles sont effacées de manière à ce qu'il ne soit pas possible de les récupérer ; les logiciels sous licence sont désinstallés.

L'effacement des supports ayant contenu des données est réalisé à l'aide d'une solution agréée par le comité de sécurité opérationnelle, adaptée à la sensibilité de ces données.

17. Sauvegarde et archivage

17.1. Politique de sauvegarde

Une politique de sauvegarde est formalisée, qui tient compte d'une part des besoins de sécurité des données, des contraintes techniques et du cadre règlementaire.

Cette politique de sauvegarde est revue au minimum une fois par an et mise à jour lors de toute évolution du système d'information.

17.2. Plan de sauvegarde

Ce plan de sauvegarde intègre les types de données suivants :

- Données utilisateur : données des utilisateurs stockées sur un serveur de fichier. Ces données ne sont pas les données stockées sur le poste de travail de l'utilisateur.
- Données applicatives : données utilisées par les applications métiers. Ces données sont généralement modifiées en permanence par les utilisateurs ou des processus applicatifs automatisés.
- Bases de données : les bases de données contiennent une grande quantité d'informations nécessaires aux applications. Ces données métiers sont constamment modifiées par les utilisateurs ou les applicatifs. Les bases de données nécessitent généralement des procédures de sauvegarde spécifiques.
- Courrier électronique des personnels : Courriers électroniques, agendas, contacts, et autres fonctionnalités de messagerie offerte aux utilisateurs.
- Applications et systèmes : données opérationnelles et environnementales avec leurs configurations respectives.

Pour chaque donnée ou ensemble de données, les besoins de sauvegarde sont établis en considérant :

- Les obligations légales, réglementaires ou contractuelles en matière de sauvegarde ou d'archivage ;
- Le temps maximal d'indisponibilité admissible, qui détermine la durée maximale pour la restauration des données et du service à partir d'une sauvegarde ;
- La perte maximale de données admissible et d'usage de l'application, qui permettront de déterminer la politique de sauvegarde (périodicité, mode opératoire).

17.3. Exigences génériques

Le plan de sauvegarde définit les conditions de sauvegarde afin de garantir une perte de données minimale en cohérence avec les besoins exprimés par les responsables d'applications.

17.3.1. Données utilisateur

Les données stockées sur les serveurs sont sauvegardées entièrement chaque semaine et une sauvegarde incrémentale est effectuée chaque jour.

Le schéma de rotation des sauvegardes permet de conserver les données pendant 12 semaines au minimum.

La sauvegarde des données stockées sur le poste de travail de l'utilisateur relève de la responsabilité de chaque utilisateur. Il est rappelé que celle-ci ne concerne pas les données sensibles qui doivent être traitées sur le serveur bureautique.

17.3.2. Données applicatives

Le schéma de rotation des sauvegardes est construit en fonction des exigences de l'application.

Par défaut, les données applicatives sont sauvegardées entièrement chaque semaine et une sauvegarde incrémentale est effectuée chaque jour.

Le plan de sauvegarde tient compte des traitements par lot réalisés au niveau des applications. Il convient de déterminer, en fonction de l'utilisation de l'application et des traitements réalisés, si la sauvegarde doit avoir lieu avant ou après les traitements qui modifient de manière importante les données applicatives.

17.3.3. Bases de données

Pour les applications sensibles, le schéma de rotation des sauvegardes est construit en fonction des exigences formulées dans le dossier de sécurité de l'application.

Par défaut, les données des bases sont sauvegardées entièrement chaque semaine et une sauvegarde incrémentale doit être faite chaque jour.

17.3.4. Courrier électronique des personnels

Les boites de courrier des personnels sont systématiquement sauvegardées.

Le plan de rotation des sauvegardes permet de conserver les données pendant 6 semaines au minimum.

17.3.5. Applications et systèmes

Les logiciels et les systèmes d'exploitation des serveurs sont sauvegardés lors de chaque modification significative (ex : mise à jour) et au minimum tous les 2 mois.

Ces sauvegardes comprennent les données de configuration des logiciels et des serveurs.

17.3.6. Contrôleurs de domaines (Active directory)

Compte tenu de leur sensibilité, les contrôleurs de domaine Active Directory sont sauvegardés dans leur intégralité au minimum 1 fois par jour.

17.4. Test des sauvegardes

Le bon déroulement des sauvegardes est validé avant stockage des supports : cette validation est effectuée soit par les moyens techniques fournis par le système de sauvegarde s'ils le permettent, soit par des vérifications manuelles.

Le volume de données sauvegardé doit être suivi par les équipes d'exploitation, pour anticiper les problèmes liés à la capacité des supports.

17.5. Restauration

Les procédures de restauration sont documentées. Des tests de restauration sont effectués au minimum 1 fois par an.

Il convient que des moyens de restauration soient également disponibles hors du site sauvegardé pour pouvoir restaurer les données en cas d'incident ayant détruit le système d'origine.

17.6. Gestion et protection des supports de sauvegarde

Les supports de sauvegarde sont conservés dans des locaux sécurisés ou des armoires fortes adaptés à leur niveau de sensibilité (équivalent à celui des données sauvegardées). Il convient que ces locaux soient suffisamment éloignés des systèmes sauvegardés pour éviter toute destruction simultanée des données et de leurs sauvegardes. Il convient d'utiliser de préférence des armoires ignifugées.

L'accès à ces locaux ou armoires fortes est limité à un nombre restreint de personnes autorisées.

17.7. Externalisation des sauvegardes

En cas d'externalisation des sauvegardes (prestataire), il convient de s'assurer par contrat que les conditions de stockage fournies par le prestataire sont conformes aux besoins exprimés par l'Université de Tours. La mise en œuvre effective des mesures de sécurité par le prestataire est contrôlée régulièrement.

18. Gestion des incidents

18.1. Organisation et procédure

18.1.1. Procédure de gestion des incidents

L'Université de Tours met en œuvre une gestion des incidents liés à la sécurité. Une organisation et des procédures sont définies, et traitent les aspects :

- Identification et caractérisation des incidents ;
- Processus de signalement des incidents ;
- Confinement de l'incident ;
- Analyse des incidents (cause, contexte), collecte de traces d'audit ;
- Planification des actions correctrices : projet et références documentaires permettant la correction ;
- Formalisation des incidents dans un référentiel unique (identification, date, circonstances, actions correctrices et références documentaires, comptes rendu) ;
- Établir des fiches reflex (réaction face à un incident connu) ;
- Incidents récurrents : prévoir un projet d'actions préventives ;
- Communication et sensibilisation des personnels.

18.1.2. Retour d'expérience

Tout incident de sécurité nécessite d'être analysé afin d'identifier les faiblesses exploitées et définir si nécessaire les mesures correctives permettant d'en limiter la répétition.

18.1.3. Conservation des traces

Tout incident de sécurité peut conduire à des sanctions, nécessiter des actions en justice ou conduire à un contentieux contractuel.

Les traces et les éléments susceptibles de servir de preuve, comme de permettre une analyse a posteriori des incidents, sont recueillis et conservés en lieu sûr.

18.2. Surveillance et signalement des incidents

18.2.1. Procédure de signalement

Il appartient au Comité de Sécurité Opérationnelle de définir et mettre en place une procédure formelle et documentée de remontée d'information et de signalement des événements et failles susceptibles d'avoir une incidence sur la sécurité des biens de l'Université de Tours.

18.2.2. Surveillance du SI et détection des incidents

Des moyens organisationnels et des outils de supervision permettent un suivi de l'activité au niveau du système d'information et la détection des incidents :

- Supervision des éléments critiques sur le plan de la sécurité (virus, passerelles de messagerie, passerelles Internet, Wifi, connexions nomades...).
- Journalisation en temps réel des évènements liés à la sécurité du système d'information.

Il appartient à la DSI :

- De réaliser une surveillance continue des systèmes et des réseaux et de revoir périodiquement les différents journaux à la recherche d'anomalies pouvant être révélatrices d'incidents.

- D'analyser et traiter les anomalies détectées. Ces analyses doivent être formalisées et conservées.

18.2.3. Cellule d'alerte et de traitement des incidents

Il appartient au Comité de Sécurité Opérationnelle de définir et mettre en place, avec le support de la DSI, une cellule en charge du traitement des alertes et des incidents liés à la SSI, tels que :

- Les intrusions dans les réseaux et les systèmes.
- Les attaques par déni de service.
- Les violations de la politique de sécurité par les utilisateurs.

Il appartient à la cellule d'alerte de définir et mettre en œuvre les procédures d'urgence afin de formaliser les actions à prendre en cas de mise en alerte pour circonstances particulières (incident d'exploitation, détection attaque, violation contrôle d'accès...).

18.2.4. Information et sensibilisation du personnel

Il appartient à chaque responsable de s'assurer que chacun, personnel ou contractant, est sensibilisé et connaît la procédure de signalement des incidents.

Le Comité de Sécurité Opérationnelle, est chargé de définir un plan d'information et de sensibilisation du personnel et de s'assurer de la mise en œuvre de cette sensibilisation par la direction des ressources humaines.

18.2.5. Signalement des incidents par le personnel

Le personnel de l'Université de Tours est tenu de signaler, le plus rapidement possible, tout événement ou faille de sécurité pouvant impacter la sécurité à son responsable hiérarchique ou au responsable sécurité désigné.

19. Gestion du plan de continuité d'activité

19.1. Organisation

Il convient d'élaborer et de gérer un processus de continuité de l'activité dans l'ensemble de l'organisme qui satisfait aux exigences en matière de sécurité de l'information requises pour la continuité de l'activité de l'organisme.

19.2. Formalisation

Il convient d'identifier les applications sensibles et leur besoin en disponibilité et les événements pouvant être à l'origine d'interruptions des processus métier tout comme la probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information.

Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.

Il convient de gérer un cadre unique pour les plans de continuité de l'activité afin de garantir la cohérence de l'ensemble des plans, de satisfaire de manière constante aux exigences en matière de sécurité de l'information et d'identifier les priorités en matière de mise à l'essai et de maintenance.

19.3. Test

Il convient de soumettre à essai et de mettre à jour régulièrement les plans de continuité de l'activité afin de s'assurer qu'ils sont actualisés et efficaces.

20. Conformité et contrôle

20.1. Conformité avec les exigences légales et réglementaires

20.1.1. Conformité avec les exigences légales et réglementaires

Les procédures de sécurité, ainsi que leurs mises à jour, sont établies dans le respect des obligations légales, règlementaires et contractuelles.

Un corpus documentaire liste l'ensemble des textes de référence encadrant les obligations légales et réglementaires. Il convient de s'y référer en cas de besoin.

20.1.2. Identification de la législation en vigueur

Une veille est assurée afin d'identifier les lois et règlements nationaux auxquels le SI de l'Université de Tours se conforme. Ces lois et règlements sont répertoriés et documentés.

Les intervenants sont régulièrement informés au travers du Comité de Sécurité Opérationnelle.

20.1.3. Respect des droits de propriété intellectuelle

L'Université de Tours dispose de règles et procédures appropriées visant à garantir le respect de la propriété intellectuelle tant pour les biens possédés ou confiés à l'Université de Tours que pour les droits détenus par l'Université de Tours.

En particulier :

- L'Université de Tours s'engage à acquérir les logiciels uniquement à partir de sources connues et réputées.
- Les licences originales et les preuves d'achats des matériels et logiciels utilisés sont conservées en lieu sûr.
- Des contrôles sont régulièrement effectués afin de vérifier le respect de la législation et de régulariser les licences globales. En cas de manquement caractérisé, des sanctions peuvent être prise à l'encontre des contrevenants.

20.1.4. Obligation de protection des enregistrements de l'organisme

Des mesures organisationnelles et techniques sont définies et mises en place afin de protéger les enregistrements importants sur un plan légal ou réglementaire (journaux de log, activités des dispositifs de contrôles d'accès, archives de vidéosurveillance) contre une perte, de destruction et falsification, conformément aux exigences légales et réglementaires et aux contraintes métier.

20.1.5. Protection des données à caractère personnel

L'Université de Tours prend en compte les exigences de la CNIL relatives à la protection des données à caractère personnel. Pour cela les actions suivantes sont menées :

- Lister les traitements de données personnelles
- Déclarer les traitements auprès de la CNIL
- Mettre en œuvre les actions d'information et de sensibilisation des acteurs concernés par les traitements d'informations personnelles
- S'assurer du non détournement de la finalité des traitements (tels que le croisement de fichiers)
- S'assurer de l'effectivité des mesures de sécurité sur les traitements, garantissant la confidentialité des données

20.1.6. Déclaration des traitements

Tout nouveau projet traitant de données à caractère personnel fait l'objet d'une information auprès d'un Correspondant Informatique et Libertés (CIL), une fiche de traitement est formalisée et validée.

20.1.7. Communication sur la protection des données à caractère personnel

Tout responsable qui souhaite mettre en œuvre un traitement de données personnelles doit préalablement contacter le Comité de Sécurité Opérationnel afin de déterminer les formalités à accomplir et les mesures à mettre en œuvre pour protéger les informations traitées.

20.2. Conformité avec les politiques et normes, conformité technique

20.2.1. Analyses de vulnérabilité

Il convient de vérifier régulièrement la conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité.

20.3. Processus d'audits internes et externes

20.3.1. Contrôle et suivi

Le Comité de Sécurité Opérationnelle fait effectuer un contrôle annuel du suivi des règles de sécurité sur au minimum 2 projets opérationnels représentatifs.

20.3.2. Réalisation des audits

Des contrôles et tests sur la base d'audit sont périodiquement réalisés à raison d'au moins une fois par an. Les audits visent à s'assurer de l'effectivité de la mise en œuvre des mesures de sécurité, et d'évaluer leur efficacité.

Les audits portent sur les aspects documentaires liés à la sécurité du SI (procédures) les aspects techniques (mesures) et organisationnels.

20.3.3. Analyse des résultats d'audit

Les résultats des audits sont analysés afin de pouvoir réviser et améliorer les procédures et les mesures de sécurité.

20.3.4. Protection des outils d'audit

Les outils d'audit (logiciels ou les fichiers de données) sont séparés des systèmes en exploitation et ne sont accessibles que par les personnes autorisées.

ANNEXE 1

1. Documents de référence :

- Politique de management de la sécurité V1.0
- Analyse de risques V1.0

2. Livrables attendus mentionnés dans la présente politique :

- Inventaire des biens du système d'information
- Procédure de mise au rebut des biens sensibles
- Chartes d'usage et de sécurité des systèmes d'information (utilisateur, administrateur, wifi, nomades, voix sur IP, étudiants...)
- Plan d'infrastructure des bâtiments et mesures de sécurité physiques
- Politique de gestion des habilitations, des profils et des droits d'accès (physiques et logiques)
- Procédure de gestion des habilitations, des profils et des droits d'accès (physiques et logiques)
- Politique de gestion des authentifiants
- Politique de sauvegarde
- Plan de sauvegarde
- Document d'application relatif à la mobilité
- Guide de bonnes pratiques de développement
- Documents d'architecture réseau
- Procédures d'administration et d'exploitation du réseau
- Politique de contrôle et filtrage des flux réseaux
- Procédures d'exploitation des systèmes informatiques
- Procédures de configuration de sécurité des serveurs et postes de travail
- Plan de gestion des mises à jour et correctifs
- Procédure de gestion des changements
- Procédure de gestion des incidents
- Inventaire des traitements de données personnelles
- Plan de formation et sensibilisation en matière de sécurité
- Politique d'utilisation des outils de cryptographie
- Programme d'audit de sécurité du système d'information
- Inventaire des équipements réseau et de sécurité non maitrisés
- Procédure de gestion et de suivi des matériels sensibles
- Politique de journalisation
- Corpus documentaire règlementaire

3. Mesures de sécurité implémentées et planifiées

Cf. Document « Plan Action ».