ADMINISTRATION

Numéro : 10.54

DIRECTIVE SUR L'UTILISATION DE L'INFONUAGIQUE

Adoption

Date :	Délibération :
2017-01-13	Comité de gestion de l'information

Modifications

Date :	Délibération :	Article(s) :
2017-07-06	Secrétariat général	6, 10
2020-03-10	Secrétariat général	7, 10
2022-10-18	Secrétariat général	Refonte

Table des matières

1. PRÉAMBULE 2
2. OBJECTIFS 2
3. CADRE NORMATIF 2
4. DÉFINITIONS 3
5. CHAMP D'APPLICATION 5
5.1 Activités 5
5.2 Utilisateurs 6
5.3 Informations institutionnelles 6
6. PRINCIPES DIRECTEURS 6
6.1 Principes généraux 6
6.2 Stockage de l'Information institutionnelle en infonuagique 7
6.3 Acquisition, mise en place et utilisation d'une solution infonuagique 7
6.4 Dépôt de documents institutionnels 8
6.5 Appareils mobiles, partage et autres Espaces de stockage 8
7. RÔLES ET RESPONSABILITÉS 8
7.1 Secrétaire général 8
7.2 Technologies de l'information 9
7.3 Officier de sécurité de l'information 9
7.4 Division de la gestion de documents et des archives (DGDA) 9
7.5 Gestionnaires d'Unités et responsables informatiques 10
7.6 Chercheurs principaux 10
7.7 Utilisateurs 11
8. MESURES TRANSITOIRES 11
9. SANCTIONS 11
10. ENTRÉE EN VIGUEUR 11
ANNEXE - TABLEAU-SYNTHÈSE DES NIVEAUX DE CONFIDENTIALITÉ 12

18 octobre 2022

Adoption

Date :	Délibération :
2017-01-13	Comité de gestion de l'information

Modifications

Date :	Délibération :	Article(s) :
2017-07-06	Secrétariat général	6, 10
2020-03-10	Secrétariat général	7, 10
2022-10-18	Secrétariat général	Refonte

1. PRÉAMBULE

Dans le cadre de ses activités et de sa mission, l'Université de Montréal détient et traite un nombre considérable d'informations, dont certaines requièrent un niveau de protection plus élevé en raison de leur valeur stratégique ou parce qu'elles contiennent des Renseignements personnels.

L'utilisation de l'Infonuagique pose des enjeux importants en matière de Sécurité de l'information. Afin de s'acquitter de ses obligations en la matière, l'Université s'est dotée de la présente Directive qui précise les modalités d'utilisation de l'Infonuagique en fonction de la valeur de l'information établie dans la Catégorisation des Actifs informationnels de l'Université. Cette Directive découle de la *Politique de sécurité de l'information* (40.28) visant une utilisation appropriée et une protection adéquate de l'Information institutionnelle tout au long de son cycle de vie.

2. OBJECTIFS

La présente Directive a pour objectifs :

- d'assurer la protection de l'Information institutionnelle, particulièrement celles ayant une valeur stratégique ou contenant des Renseignements personnels ;
- de mettre en œuvre un cadre normatif interne afin de soutenir et d'encadrer les Unités et les Utilisateurs en ce qui concerne l'utilisation de l'infonuagique pour l'enseignement, la recherche et l'administration de l'Université ;
- d'encadrer l'accès et la mise en place de solutions infonuagiques offrant une assurance raisonnable de conformité à l'égard du cadre normatif institutionnel et des lois, directives et pratiques gouvernementales en la matière.

3. CADRE NORMATIF

La présente Directive s'inscrit dans un contexte régi notamment par :

- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q., c. G-1.03) ;
- la *Loi concernant le cadre juridique des technologies et l'information* (L.R.Q., c. C-1.1) ;

- la *Loi sur l'accès aux documents des organismes publics et sur la protection des Renseignements personnels* (RLRQ c. A-2.1) ;
- la *Loi sur les archives* (L.R.Q. c. A-21.1) ;
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics* (Décret no 261-2012 du 28 mars 2012) ;
- la *Directive sur la sécurité de l'information gouvernementale* (Décret 7-2014 du 15 janvier 2014) ;
- le *Cadre gouvernemental de gestion de la sécurité de l'information* (juin 2014).

À ce cadre juridique, s'ajoutent des politiques internes mises en œuvre par l'Université, soit :

- Politique de sécurité de l'information (40.28) ;
- Politique de gestion de l'information (10.47) ;
- Politique sur la gestion de documents et des archives (10.49) ;
- Politique sur la protection des renseignements personnels (40.29).

4. DÉFINITIONS

Aux fins de la présente Directive, on entend par :

Actif informationnel : une information, un système ou une technologie de l'information.

Catégorisation des Actifs informationnels : évaluation des Actifs informationnels en fonction de l'importance de l'Information qu'ils comportent, des obligations de l'Université et de l'impact d'un incident pour celle-ci.

Confidentialité : propriété d'une Information qui n'est accessible qu'aux personnes ou entités désignées et autorisées, et qui n'est divulguée qu'à celles-ci.

Cycle de vie de l'information : ensemble des étapes que franchit une Information et qui vont de sa création ou de sa collecte, en passant par son enregistrement, son transfert, son utilisation, son traitement et sa communication, jusqu'à sa conservation permanente ou sa destruction, notamment en conformité avec le calendrier de conservation de l'Université.

Détenteur de l'information : toute personne qui, dans le cadre de ses fonctions, conserve l'Information que l'Université détient dans l'accomplissement de sa mission, ainsi que les ressources qui la sous-tendent.

Document : un document est constitué d'Information portée par un support. L'Information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'Information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles réinscriptibles sous l'une de ces formes ou en un autre système de symboles.

Document institutionnel : document, quels que soient sa date, sa nature ou son support, produit ou reçu par l'Université, une de ses Unités ou un de ses employés dans l'exercice de ses fonctions (ex. : un rapport d'activité, une demande de poste, un procès-verbal, un dossier étudiant, un courriel faisant état d'une demande de services, etc.).

Espace de stockage : terme générique employé pour désigner une infrastructure utilisée pour le stockage d'information.

Infonuagique : modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet d'accéder, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation.

Information : renseignements consignés sur un support quelconque pour être conservés, traités ou communiqués comme éléments de connaissance.

Information institutionnelle : information utilisée dans le cadre des activités d'enseignement, de recherche et d'administration de l'Université.

Information institutionnelle confidentielle : information dont l'accès et l'utilisation sont réservés à des personnes ou des entités désignées et autorisées parce qu'elle contient des éléments stratégiques ou des Renseignements personnels dont la divulgation non autorisée risquerait de causer des préjudices négligeables, faibles ou modérés à l'Université, à ses partenaires ou à des individus (étudiants, employés, clients des cliniques, locataires des résidences, abonnés des bibliothèques, abonnés des services sportifs, participants à des projets de recherche ou autres).

Information institutionnelle hautement confidentielle : information dont l'accès et l'utilisation sont réservés à des personnes ou des entités désignées et autorisées parce qu'elle contient des éléments stratégiques ou des **Renseignements personnels sensibles** dont la divulgation non autorisée risquerait de causer des préjudices élevés ou critiques à une Unité ou à l'ensemble de l'Université, à ses partenaires ou à des individus (étudiants, employés, clients des cliniques, locataires des résidences, abonnés des bibliothèques, abonnés des services sportifs, participants à des projets de recherche ou autres), notamment le numéro d'assurance sociale, le dossier santé, les cartes de paiement, etc.

Information institutionnelle non confidentielle : information dont l'accès et l'utilisation ne sont pas restreints puisqu'elle ne contient aucun élément stratégique ni Renseignement personnel.

Renseignement personnel : toute information qui concerne une personne physique et qui peut permettre de l'identifier :

- directement, c'est-à-dire par le recours à cette seule information ; ou
- indirectement, c'est-à-dire par recoupement avec d'autres informations.

Renseignement personnel sensible : tout renseignement personnel qui, de par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée.

Sécurité de l'information : protection de l'Information et des Actifs informationnels contre les risques et les incidents.

Synchronisation : service applicatif qui permet de maintenir à jour, de façon unidirectionnelle ou bidirectionnelle, un fichier dupliqué et stocké dans différents endroits ou appareils (portable, tablette, téléphone, etc.) en répliquant simultanément sur chacun de ceux-ci les modifications qui y sont apportées.

Système officiel de classification (SOC) : ensemble de conventions, de méthodes et de procédures structurées permettant aux Unités de l'Université de classifier, indexer et classer de façon uniforme et systématique leurs Documents institutionnels.

Unité : l'un ou l'autre des facultés, écoles, départements, services administratifs, ainsi que l'une ou l'autre des unités de recherche constituées par le Comité Exécutif de l'Université.

Université : l'Université de Montréal, excluant ses écoles affiliées.

Utilisateurs : les personnes physiques et morales visées par la présente directive, telles qu'énumérées à l'article 5.2.

5. CHAMP D'APPLICATION

5.1 Activités

Les activités visées sont celles portant sur l'utilisation de l'infonuagique pour l'enseignement, la recherche et l'administration de l'Université.

5.2 Utilisateurs

Les utilisateurs sont :

- les personnes à l'emploi de l'Université ;
- les Unités de l'Université ;
- tout consultant, fournisseur, partenaire, invité, organisme, firme externe ou autre tiers ayant accès aux systèmes d'information de l'Université et autorisés à accéder, à exploiter ou à héberger l'Information informationnelle de l'Université.

5.3 Informations institutionnelles

Les Informations institutionnelles sont celles :

- détenues par l'Université ;
- détenues par un fournisseur infonuagique au bénéfice ou pour et au nom de l'Université ;
- utilisées par un consultant, un fournisseur, un partenaire, un organisme ou une firme externe et détenues chez un fournisseur infonuagique au bénéfice ou pour et au nom de l'Université.

6. PRINCIPES DIRECTEURS

6.1 Principes généraux

- L'utilisation d'une solution Infonuagique doit offrir un niveau adéquat de protection de l'information à caractère personnel, confidentiel et/ou essentiel au fonctionnement de l'organisation ;
- L'utilisation d'une solution Infonuagique doit se faire de manière à se conformer à l'environnement réglementaire de l'organisation ;
- L'utilisation d'une solution Infonuagique doit permettre l'élimination des données de manière fiable et sécuritaire et ce, au moment où ils doivent l'être, en fonction des normes, politiques et procédures.

6.2 Stockage de l'Information institutionnelle en infonuagique

- Le choix de l'Espace de stockage et les normes de Sécurité de l'information sont déterminés par la valeur de l'information établie selon la Catégorisation des Actifs informationnels de l'Université, laquelle comporte 3 niveaux de confidentialité : Information non confidentielle, Information confidentielle et Information hautement confidentielle (voir le tableau-synthèse en annexe) ;

- Aucun Renseignement personnel, Information confidentielle ou hautement confidentielle ne doit être stocké dans une solution infonuagique dont les serveurs sont situés à l'extérieur du Canada sans le consentement du Secrétaire général de l'Université ;

- L'Information hautement confidentielle ne peut être stockée dans une solution infonuagique que si celle-ci a fait l'objet d'une évaluation de sécurité spécifique par les TI ; cette évaluation est requise pour que soit approuvée l'utilisation de ladite solution pour le stockage de l'Information hautement confidentielle et pour s'assurer que cette information soit considérée comme étant adéquatement protégée ; si la solution change sur le plan matériel, une réévaluation de sécurité spécifique par les TI est requise ;

- Lorsque l'information hautement confidentielle est transmise par courriel, elle doit être protégée par chiffrement ; la clé (mot de passe) doit être transmise au destinataire de manière distincte ;

- Aucun Renseignement personnel, Information confidentielle ou hautement confidentielle ne doit être stocké dans une solution infonuagique non homologuée par les TI.

6.3 Acquisition, mise en place et utilisation d'une solution infonuagique

- L'acquisition, la mise en place et l'utilisation d'une solution infonuagique doit respecter les normes de sécurité de l'information prescrites par les Technologies de l'information (TI) de l'Université et faire l'objet d'une approbation par les TI et le Secrétariat général ;

- L'acquisition et la mise en place d'une solution infonuagique, comme pour tout service informatique, doit faire l'objet d'une évaluation de sécurité et, s'il elle implique des renseignements personnels ou si elle risque d'avoir une incidence sur le respect de la vie privée des personnes, d'une Évaluation des facteurs relatifs à la vie privée (EFVP) ;

- Lors de l'acquisition et de la mise en place d'une solution infonuagique, les clauses contractuelles doivent prévoir la protection de l'information, dont la protection des renseignements personnels, dans le respect du cadre législatif s'appliquant à l'Université ;

- Même si la solution infonuagique est gratuite, le fournisseur devient un fournisseur de l'Université et la signature d'un contrat est requise ;

- Pour les données de recherche, le chercheur principal est responsable et imputable du choix de la solution infonuagique qu'il effectue.

6.4 Dépôt de documents institutionnels

6.4.1 Aucun Document institutionnel contenant des Informations confidentielles ou hautement confidentielles ne doit être stocké dans une solution infonuagique non homologuée par les TI.

6.4.2 Les versions finales des Documents institutionnels doivent être stockées dans un dépôt documentaire sécurisé homologué par les TI (DocUM, SyGED) et structurées conformément au Système officiel de classification (SOC), de façon à assurer la gestion de leur cycle de vie, sauf dans les cas où les documents sont utilisés à l'intérieur d'une plateforme institutionnelle (exemple : Synchro) ;

6.5 Appareils mobiles, partage et autres Espaces de stockage

- La synchronisation de toute information institutionnelle hautement confidentielle est interdite, incluant sur les appareils mobiles, portables et autres Espaces de stockage ;

- La synchronisation de toute information qui n'est pas hautement confidentielle s'effectue en utilisant le système de gestion des identités et des accès de l'Université ;

- L'accès et l'utilisation de tout appareil (ordinateur de bureau, portable, tablette, téléphone intelligent) institutionnel ou personnel pour traiter de l'information institutionnelle doivent être protégés par des mécanismes de sécurité (système de gestion des identités et des accès de l'Université, code d'accès (PIN), empreinte digitale, reconnaissance vocale) et autres bonnes pratiques en matière de Sécurité de l'information.

7. RÔLES ET RESPONSABILITÉS

Les rôles et les responsabilités des différents intervenants en matière de Sécurité de l'information sont les suivants :

7.1 Secrétaire général

Le Secrétaire général assume le rôle de Responsable organisationnel de la Sécurité de l'information (ROSI) au sein de l'Université. À cet égard, il :

- est responsable de l'application de la présente directive ;

- s'assure que les ententes de services et les contrats conclus avec des fournisseurs, des partenaires, des consultants et des organismes externes sont conformes à la présente directive et aux exigences en matière de Sécurité de l'information.

7.2 Technologies de l'information

Les TI s'assurent de la prise en charge des exigences de Sécurité de l'information dans l'exploitation des systèmes d'information, ainsi que lors de la réalisation de projets de développement et de l'acquisition de systèmes d'information.

7.3 Officier de sécurité de l'information

L'officier de sécurité de l'information :

- conçoit et met en œuvre l'architecture de Sécurité de l'information et arrime les solutions retenues aux processus organisationnels de Sécurité de l'information ;

- assiste les Détenteurs de l'Information en matière d'analyse des risques de Sécurité de l'information sous leur responsabilité ;

- contribue au processus d'acquisition de biens et de services pour s'assurer que les ententes de services et les contrats intègrent des dispositions afin de respecter les exigences en matière de Sécurité de l'information ;

- collabore à l'élaboration du contenu du programme de sensibilisation et d'information en matière de Sécurité de l'information.

7.4 Division de la gestion de documents et des archives (DGDA)

La DGDA :

- produit et met à jour la Catégorisation des Actifs informationnels de l'Université ;

- sensibilise, informe et assiste les Utilisateurs et les Unités dans la mise en application de la Catégorisation des Actifs informationnels de l'Université.

7.5 Gestionnaires d'Unités et responsables informatiques

Les gestionnaires d'Unités, et les responsables informatiques :

- identifient la valeur de l'information en fonction de la Catégorisation des Actifs informationnels de l'Université ;
- informent le personnel relevant de leur autorité de la présente directive afin de le sensibiliser à la nécessité de s'y conformer ;
- protègent l'Information institutionnelle sous leur responsabilité, en s'assurant que celles-ci sont utilisées par le personnel relevant de leur autorité en conformité avec le cadre normatif ;
- s'assurent que les exigences en matière de Sécurité de l'information sont prises en compte dans tout processus d'acquisition et contrat de service sous leur responsabilité, et voient à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engagent à respecter et respectent la présente directive et le cadre normatif en matière de Sécurité de l'information ;
- rapportent au Secrétaire général tout problème lié à l'application de la présente directive ;
- rapportent aux TI tout incident afférant à la Sécurité de l'information.

7.6 Chercheurs principaux

Les chercheurs principaux :

- identifient la valeur de l'information en fonction de la Catégorisation des Actifs informationnels de l'Université ;
- informent les équipes relevant de leur autorité de la présente directive afin de les sensibiliser à la nécessité de s'y conformer ;
- protègent l'Information institutionnelle sous leur responsabilité, en s'assurant que celles-ci sont utilisées en conformité avec le cadre normatif ;
- s'assurent que les exigences en matière de Sécurité de l'information sont prises en compte dans tout processus d'acquisition et contrat de service sous leur responsabilité, et voient à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engagent à respecter et respectent la présente directive et le cadre normatif en matière de Sécurité de l'information ;

- rapportent au Secrétaire général tout problème lié à l'application de la présente directive ;

- rapportent aux TI tout incident afférant à la Sécurité de l'information.

7.7 Utilisateurs

Tout Utilisateur qui accède à de l'Information, la consulte ou la traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger cette Information.

À cette fin, il doit :

- se conformer à la présente Directive ;

- utiliser les solutions infonuagiques mises à sa disposition en respectant les règles de sécurité établies dans la présente Directive, lesquelles tiennent compte de la valeur de l'information établie dans la Catégorisation des Actifs informationnels de l'Université ;

- signaler aux TI tout incident susceptible de constituer une contravention à la présente directive ou de constituer une menace à la Sécurité de l'information de l'Université.

8. MESURES TRANSITOIRES

Toutes les Informations institutionnelles contenant des Renseignements personnels ou confidentiels, et prioritairement les Informations hautement confidentielles, actuellement stockées dans une solution infonuagique non homologuée par les TI doivent être déplacées dans une solution institutionnelle approuvée. Le choix de l'Espace de stockage doit être fait en fonction de la valeur de l'information établie dans la Catégorisation des Actifs informationnels de l'Université. Les copies stockées dans les solutions infonuagiques non homologuée par les TI doivent être détruites.

9. SANCTIONS

Toute personne qui enfreint la présente Directive est passible de sanctions selon le cadre normatif applicable.

10. ENTRÉE EN VIGUEUR

La présente Directive entre en vigueur lors de son adoption par le Comité de direction.

18 octobre 2022

ANNEXE
TABLEAU-SYNTHÈSE DES NIVEAUX DE CONFIDENTIALITÉ

INFORMATION NON CONFIDENTIELLE | RISQUE FAIBLE		
Définition	**Exemples**	**Risques potentiels**
- Aucun Renseignement personnel - Informations n'ayant aucune valeur stratégique pour l'Université - Les Information non confidentielles peuvent être librement divulguées ou, dans certains cas, leur divulgation pourrait causer un préjudice minime	- Informations **publiques** : informations publiées sur le site Web public de l'Université, noms et coordonnées professionnelles des membres du corps professoral et du personnel administratif de l'Université, programme d'une collation de grades, guide de bourses, convention collective en vigueur, rapport annuel, calendrier universitaire, revue de presse, support de cours partagés comme une ressource éducative libre, etc. - Informations **internes** : statistiques, listes et inventaires, règlements et politiques en cours d'élaboration ou de révision, calendriers d'activités, documents relatifs aux relations entretenues par l'unité avec d'autres unités de l'UdeM, descriptions de fonctions et de tâches, guides de formation, liste des cours ou événements par locaux, inventaire des biens, modèles et formulaires, communiqués internes, données de recherche dont le partage n'est pas soumis à des restrictions légales ou contractuelles, etc.	- Perturbations opérationnelles mineures

Adoption

Date :	Délibération :
2017-01-13	Comité de gestion de l'information

Modifications

Date :	Délibération :	Article(s) :
2017-07-06	Secrétariat général	6, 10
2020-03-10	Secrétariat général	7, 10
2022-10-18	Secrétariat général	Refonte

INFORMATION CONFIDENTIELLE | RISQUE MODÉRÉ		
Définition	**Exemples**	**Risques potentiels**
- Renseignements personnels non sensibles - Informations ayant une valeur stratégique modérée pour l'UdeM - Les Informations confidentielles doivent être protégées en vertu des lois applicables et du cadre normatif contre tout accès, utilisation ou destruction non autorisés. La divulgation d'informations confidentielles à des personnes non autorisées pourrait causer des préjudices modérés à l'Université ou à d'autres personnes.	- Informations concernant le **parcours académique d'un étudiant** : travaux et examens complétés, résultats académiques, relevés de notes, dossier étudiant ne contenant pas d'information sur la santé, etc. - **Identification de personnes sans renseignement personnel sensible** : matricule d'un étudiant ou d'un employé, coordonnées personnelles (adresse, numéro de téléphone), liste d'inscriptions à un cours, répartition des tâches d'enseignement, liste de chargé(e)s de cours et auxiliaires d'enseignement, liste et coordonnées des invités à un événement, documents de saisie et de vérification de la gestion du temps des employés (feuilles de temps, feuilles de présence, fiche d'assiduité), etc. - Informations exclusives reçues d'un tiers dans le cadre d'un accord de non-divulgation - Revues de bibliothèque à diffusion restreinte - Informations et dossiers financiers confidentiels - Données de recherche qui ne sont pas prêtes à être partagées ou dont l'accès est soumis à des restrictions légales ou contractuelles, mais dont les conséquences d'un incident de confidentialité sont mineures pour les participants, les chercheurs ou l'Université	- Préjudice modéré à une ou plusieurs personnes, impact modéré sur la réputation ou les opérations de l'Université, perte financière modérée, telle que les amendes réglementaires

Adoption

Date :	Délibération :
2017-01-13	Comité de gestion de l'information

Modifications

Date :	Délibération :	Article(s) :
2017-07-06	Secrétariat général	6, 10
2020-03-10	Secrétariat général	7, 10
2022-10-18	Secrétariat général	Refonte

INFORMATION HAUTEMENT CONFIDENTIELLE | RISQUE ÉLEVÉ		
Définition	**Exemples**	**Risques potentiels**
- Renseignements personnels sensibles - Informations ayant une valeur stratégique élevée pour l'UdeM - Les Informations hautement confidentielles doivent être protégées en vertu des lois applicables et du cadre normatif contre tout accès, utilisation ou destruction non autorisés. La divulgation d'Informations hautement confidentielles à des personnes non autorisées pourrait causer des préjudices sérieux à l'Université ou à d'autres personnes	- **Renseignements personnels sensibles** : numéro d'assurance sociale, date de naissance, données biométriques, données génétiques, origine ethnique, orientation sexuelle, données de géolocalisation, opinions de participants à la recherche, numéro de permis de conduire, passeport, document d'immigration, dossier d'admission, dossier d'un employé, demande d'honoraire professionnel contenant un numéro d'assurance sociale, etc. - Informations concernant **la santé physique et mentale d'une personne** (étudiant, employé, patient, participant à la recherche ou autre) : dossier d'un patient d'une clinique médicale, dossier étudiant contenant des informations sur la santé, dossier d'étudiant en situation de handicap, évaluation de la condition de santé ou de la forme physique, documents relatifs à un congé de maternité, etc. - Informations concernant **la situation financière d'une personne** (étudiant, employé, patient, participant à la recherche ou autre) : salaire d'un employé, demande d'aide financière, dossier d'un boursier, informations sur le compte bancaire (par exemple, les détails du dépôt direct), informations relatives à une carte de paiement, etc. - Informations concernant **des enquêtes en cours** : cas de plagiat, cas de différend, plainte à l'ombudsman, plainte en matière de harcèlement, cas de discipline, demande auprès des services juridiques, griefs, mesures disciplinaires, allégation de manquement à la conduite responsable en recherche, etc.	- Préjudice sérieux à une ou plusieurs personnes, vol d'identité, violation de la vie privée, impact grave sur la réputation ou les opérations de l'Université, poursuites judiciaires, perte financière importante, telle que des amendes réglementaires ou des dommages-intérêts résultant d'un litige