UQAR Université du Québec à Rimouski

TITRE : **DIRECTIVE SUR L'ACQUISITION, LA REFONTE ET LA MISE A JOUR DES SYSTEMES D'INFORMATION**

APPROUVÉ PAR: **COMITÉ EXÉCUTIF** CODE : **C3-D39**

EN VIGUEUR : 16-12-2025 RÉS. : EX-905-7103 16-12-2025

RESPONSABILITÉ : SECRETARIAT GENERAL

RÉVISION PRÉVUE : 2028

TABLE DES MATIÈRES

1 PRÉAMBULE

Dans le cadre de sa mission et de ses activités, l'Université doit collecter et traiter un ensemble de données pouvant contenir des renseignements personnels. Ces renseignements sont conservés sur des supports variés et peuvent faire l'objet d'un traitement à l'intérieur d'un système d'information.

Par sa nature, un système d'information peut engendrer des risques quant à la sécurité de l'information, la protection des renseignements personnels et sur le respect de la vie privée. Afin de respecter les obligations de protection des données sous sa responsabilité, l'UQAR doit s'assurer que les systèmes d'information déployés fassent l'objet des vérifications nécessaires dans le but d'assurer une protection adéquate de l'information détenue par l'Université et le respect de la vie privée des personnes concernées par celle-ci.

2 OBJECTIFS

La présente directive a pour but d'assurer que les principes de sécurité de l'information et de protection des renseignements personnels soient respectés à toute étape de l'utilisation d'un système d'information nécessaire à la mission ou aux activités de l'Université.

Ces principes seront analysés selon la nature et la quantité de l'information concernée, du contexte applicable et de l'utilisation prévue du système d'information. Les conclusions et mesures d'atténuation seront consignées dans l'analyse SI-PRP. La présente directive prévoit ainsi les modalités applicables en vue de l'acquisition, la refonte ou la mise à jour d'un système d'information nécessaire à la mission ou aux activités de l'Université. Elle précise, notamment, les modalités et la procédure et les actions préalables à réaliser par les personnes impliquées.

Les processus décrits à la présente directive sont complémentaires au processus de priorisation prévu à la Directive encadrant la gestion des projets en ressources informationnelles et s'exécutent simultanément.

3 CADRE JURIDIQUE

La présente directive est élaborée en tenant compte du cadre juridique suivant :

- Loi sur l'Université du Québec (RLRQ, ch. U-1);
- Charte des droits et libertés de la personne (RLRQ, ch. C-12);
- Code civil du Québec (RLRQ,, ch. CCQ-1991);
- Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, ch. G-1.03);
- Loi concernant le cadre juridique des technologies et l'information (RLRQ, chapitre C-1.1);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1);
- Loi sur les archives (RLRQ, chapitre A-21.1);
- Loi canadienne sur les droits de la personne (LRC, 1985, chapitre H-6);
- Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, r. 02);
- Directive sur la sécurité de l'information gouvernementale;
- Règlement 15 : Registres officiels et documentation administrative de l'Université;
- C3-D99 Politique sur la sécurité de l'information;

- C3-D109 Cadre de gestion de la sécurité de l'information;
- C3-D111 Politique établissant le cadre de gouvernance en matière de protection des renseignements personnels
- C3-D112 Directive sur la collecte, l'utilisation et la communication de renseignements personnels
- Directive encadrant la gestion des projets en ressources informationnelles – À venir.

4 CHAMPS D'APPLICATION

La présente directive s'adresse principalement aux personnes membres de la communauté universitaire qui sont impliquées dans le processus visant l'acquisition, la refonte ou la mise à jour d'un système d'information.

La présente directive s'adresse également aux membres de la communauté universitaire qui souhaitent déposer une demande pour faire l'acquisition d'un système d'information nécessaire à la mission ou aux services offerts par l'Université, c'est-à-dire, sans s'y limiter, le personnel cadre, les professeures et professeurs, les personnes chargées de cours, le personnel administratif et de soutien, les personnes étudiantes de même que toute personne physique ou morale qui agit à l'Université à titre de personne consultante, de partenaire ou à titre de fournisseur de services.

5 DÉFINITIONS

Aux fins de la présente directive, les termes suivants se définissent comme suit :

Acquisition d'un système d'information : aux fins de la présente directive, l'acquisition désigne toute démarche visant à acheter, implanter, programmer ou autrement obtenir un système d'information incluant, notamment, tous les projets issus d'un dossier d'opportunité et les demandes individuelles visant l'acquisition d'un système d'information pour répondre à un besoin spécifique ou ponctuel.

Analyse de sécurité : analyse effectuée par l'équipe de sécurité du Service des technologies de l'information ayant pour objectif d'identifier les risques en matière de sécurité de l'information et de cybersécurité.

Analyse SI-PRP : désigne le cumul de l'évaluation des facteurs relatifs à la vie privée et de l'analyse de sécurité produites pour un projet d'acquisition, de refonte ou de mise à jour d'un système d'information.

Évaluation des facteurs relatifs à la vie privée (EFVP) : désigne la démarche préventive obligatoire qui vise à mieux protéger les renseignements personnels et à respecter davantage la vie privée des personnes physiques.

Mise à jour d'un système d'information : implique le développement ou la mise à jour des fonctionnalités principales d'un système d'information. La mise à jour doit entrainer des modifications significatives du traitement des données au sein du système d'information. Une mise à jour peut consister dans :

- l'ajout d'un module impliquant le traitement d'information
- l'ajout ou changement du lieu d'hébergement des données
- l'ajout de formulaires électroniques collectant des renseignements.

Constitue également une mise à jour du système d'information le fait de modifier les conditions, le contexte et la portée de l'utilisation d'un système d'information.

Refonte d'un système d'information : la refonte implique des modifications ou des changements majeurs à l'objectif ou aux fonctionnalités principales du système d'information, contrairement à la mise à jour.

Renseignement personnel : désigne les renseignements qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement concernant cette personne ou lorsque sa seule mention révèlerait un renseignement personnel la concernant.

Sont notamment du domaine public et ne sont pas considérés comme personnels les renseignements suivants :

- nom, titre, fonction, classification, traitement, l'adresse et le numéro de téléphone professionnels d'un membre du personnel d'un organisme public;
- un renseignement concernant une personne en sa qualité de partie à un contrat de service conclu avec un organisme public.

Renseignement personnel sensible : désigne un renseignement personnel qui, notamment par sa nature 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 respect de la vie privée.

Support : moyen de conservation et de diffusion d'information autre qu'un système d'information. Un support peut être numérique (clé USB, cartes mémoires, appareils mobiles, bande de copie, disque externe, vidéo, etc.) ou papier.

Système d'information : ensemble organisé de moyens mis en place pour recueillir, stocker, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un objectif ou besoin déterminé, y incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions. Un fichier ou document individualisé n'est pas un système d'information en soi.

Il peut s'agir entre autres d'un :

- système informatique de traitement des dossiers;
- logiciel de vidéoconférence ou de collaboration;
- système biométrique;
- système d'intelligence artificielle (IA);
- système de cartes à puce/RFID;
- système de vidéosurveillance;
- système statistique;
- système de gestion de la paie;
- d'un dossier électronique;
- d'une application mobile;
- d'un site Web.

6 RÔLES ET RESPONSABILITÉ

6.1 Personne responsable de la protection des renseignements personnels et personne cheffe de la sécurité de l'information organisationnelle (personne RPRP-CSIO)

La personne RPRP-CSIO s'assure que toute acquisition, refonte ou mise à jour d'un système d'information respecte les règles de protection de renseignements personnels et de sécurité de l'information applicables à l'Université.

Elle s'assure ainsi que les conclusions et mesures d'atténuation identifiées à l'analyse SI-PRP sont respectées, notamment qu'elles sont adéquatement mises en œuvre et maintenues tout au long du cycle de vie du système d'information.

En cas d'analyse SI-PRP défavorable, la personne RPRP-CSIO peut demander des corrections ou refuser l'acquisition, la refonte ou la mise à jour du système d'information visé. Dans le cas où les mesures d'atténuation identifiées à l'analyse SI-PRP ne sont pas respectées en cours d'utilisation du système d'information, la personne RPRP-CSIO peut également exiger que l'utilisation soit suspendue le temps d'apporter les correctifs nécessaires.

En vue de la mise en œuvre de la présente directive, la personne RPRP-CSIO peut déléguer tout pouvoir à une personne membre de l'équipe PRP.

6.2 Service des technologies de l'information

Les personnes membres du Service des technologies de l'information (STI), en fonction de leurs rôles et responsabilités respectifs, s'assurent de faire cheminer toute demande d'acquisition, de refonte ou de mise à jour d'un système d'information conformément à la présente directive et au processus de priorisation en vigueur à l'Université. Elles s'assurent également que l'analyse SI-PRP est demandée en temps opportun.

Les membres de l'équipe de sécurité au STI réalisent les analyses de sécurité et s'assurent que le système d'information visé respecte les exigences en matière de sécurité de l'information et de cybersécurité et émettent les conclusions et mesures d'atténuation nécessaires.

6.3 Service des finances et des approvisionnements et personnes signataires autorisées

Les personnes membres du Service des finances et des approvisionnements et les personnes signataires autorisées sont chargées, dans le cadre du processus d'approvisionnement, d'effectuer l'acquisition du système d'information par contrat, par signature d'un bon de commande ou, pour les projets de plus grande envergure qui le nécessitent, par appel d'offres.

Afin d'assurer le respect des principes de la présente directive, ces personnes doivent, avant d'approuver un bon de commande, de signer un contrat ou de lancer un processus d'appels d'offres, s'assurer que les étapes préalables à cette acquisition ont été respectées et qu'une analyse SI-PRP favorable a été produite.

Si aucune analyse SI-PRP n'a été produite, ou s'il est porté à l'attention de ces personnes qu'une étape préalable n'a pas été respectée, celles-ci doivent mettre en pause l'acquisition du système d'information et rediriger la demande vers la personne appropriée.

6.4 L'équipe chargée de la protection des renseignements personnels

L'équipe chargée de la protection des renseignements personnels (L'équipe PRP) est composée, notamment :

- de la personne responsable de la protection des renseignements personnels;
- d'une conseillère ou d'un conseiller juridique;
- d'une conseillère ou d'un conseiller en sécurité de l'information et protection des renseignements personnels;
- d'une ou d'un archiviste.

Les membres de l'équipe PRP collaborent à la réalisation des évaluations des facteurs relatifs à la vie privée, s'assurent que le système d'information visé respecte le cadre légal et administratif applicable à l'Université et émettent les conclusions et mesures d'atténuation nécessaires.

6.5 Personnes demanderesses

Toute personne effectuant une demande d'acquisition, de refonte ou de mise à jour d'un système d'information s'assure que les dispositions de la présente directive ont été respectées, notamment qu'une analyse SI-PRP favorable a été produite.

Ces personnes s'assurent également de mettre en œuvre les mesures d'atténuation identifiées en application de la présente directive lorsqu'elles les concernent.

7 PRINCIPES DIRECTEURS

Tout système d'information doit respecter les règles de protection des renseignements personnels et de sécurité de l'information applicables à l'Université. À cet effet, avant d'être autorisée, l'acquisition, la refonte ou la mise à jour d'un système d'information doit faire l'objet d'une analyse SI-PRP favorable.

8 DEMARCHE VISANT L'OBTENTION D'UNE ANALYSE SI-PRP FAVORABLE

Toute demande d'acquisition, de refonte ou de mise à jour de système d'information doit être soumise à la personne appropriée au STI, selon le processus établi.

Si nécessaire, la personne responsable au STI fait cheminer celle-ci selon les principes de priorisation en vigueur à l'Université. Celle-ci s'assure également que la démarche visant l'obtention d'une analyse SI-PRP est entamée au tout début du processus de priorisation des projets impliquant des ressources informationnelles.

La démarche d'obtention de l'analyse SI-PRP n'a pas pour effet de suspendre le cheminement de la demande d'acquisition, de refonte ou de mise à jour du système d'information. Toutefois, aucun bon de commande ou contrat ne peut être émis ou signé pour l'acquisition, la refonte ou la mise à jour d'un système d'information tant que l'analyse SI-PRP favorable n'a pas été obtenue et qu'il a été démontré que les mesures d'atténuation de cette analyse seront mises en œuvre.

Toute demande qui ne respecte pas les conditions prévues au présent article doit être refusée ou redirigée.

9 ANALYSE SI-PRP

La demande d'analyse SI-PRP est obligatoire, et ce, pour tout type de projet dans toute démarche d'acquisition, de refonte ou de mise à jour d'un système d'information. La portée de cette analyse sera proportionnelle à la nature et à la sensibilité du projet.

La demande d'analyse SI-PRP doit être réalisée en début de démarche. Dans la mesure où la démarche n'identifie pas un système d'information en particulier, l'analyse SI-PRP sera produite sous une forme préliminaire en identifiant les enjeux à tenir en compte lors du choix du système d'information. La version finale de l'analyse SI-PRP sera produite en tenant compte du choix final du système d'information.

L'analyse SI-PRP aura l'une des conclusions suivantes :

- évaluation favorable – aucune mesure d'atténuation n'est nécessaire
- évaluation favorable conditionnelle à la mise en œuvre des mesures d'atténuation
- évaluation défavorable

Si l'analyse SI-PRP est défavorable, la demande d'acquisition, de refonte ou de mise à jour du système d'information doit être refusée. De même, si les mesures d'atténuation identifiées dans une évaluation favorable conditionnelle ne sont pas acceptées par le partenaire ou si celles-ci ne sont pas respectées, la personne RPRP-CSIO peut refuser la démarche.

L'analyse SI-PRP est évolutive tout au long du cycle de vie du système d'information tant que le système d'information est actif, c'est-à-dire que les conclusions et mesures d'atténuation y étant identifiées sont sujettes à être modifiées lorsque le projeta démarche d'acquisition, de mise à jour ou de refonte d'un système d'information fait l'objet de changements, notamment en lien avec la nature et la quantité de l'information traitée, les conditions, le contexte et la portée de l'utilisation du système d'information, les personnes qui y auront accès ou en cas de modifications au cadre légal et règlementaire.

9.1 Analyse de sécurité

Faisant partie de l'analyse SI-PRP, l'analyse de sécurité a pour objectif d'identifier les risques associés au système d'information visé au regard de la sécurité de l'information et de la cybersécurité.

La portée de l'analyse de sécurité doit être proportionnelle à la sensibilité du projet. Cette proportionnalité est établie en fonction, notamment, des éléments suivants :

- de la criticité du système d'information et des données impliquées;
- de la sensibilité des données impliquées;
- du nombre de personnes utilisatrices;
- du type d'hébergement (infonuagique, sur site, etc.);
- de la présence ou l'absence d'une entente contractuelle avec le fournisseur;
- de la réputation ou de l'historique du fournisseur auprès de l'établissement Université ou du réseau de l'enseignement supérieur;
- de l'utilisation de technologies émergentes (IA, chaine de blocs, etc.);
- de la nature du système d'information et de l'utilisation prévue;
- des mesures de protection ou d'atténuation déjà en place;
- des éléments propres au contexte de la demande.

9.2 Évaluation des facteurs relatifs à la vie privée

Faisant partie de l'analyse SI-PRP, L'EFVP a pour objectif d'identifier les risques associés au système d'information au regard de la protection des renseignements personnels et des attentes en matière de vie privée.

La portée de l'EFVP doit être proportionnelle à la sensibilité du projet. Cette proportionnalité est établie en fonction, notamment, des éléments suivants :

- du nombre de renseignements personnels impliqués
- de la sensibilité des renseignements personnels impliqués
- de la finalité et de l'utilisation prévue des renseignements personnels impliqués
- de la nature du système d'information
- des mesures de protection ou d'atténuation déjà en place
- des éléments propres au contexte de la demande.

10 REGISTRE DES ANALYSES SI-PRP

Les membres de l'équipe PRP et de l'équipe de sécurité du STI inscrivent toute demande d'analyse SI-PRP dans le registre approprié. Celui-ci doit être présenté au Comité sur l'accès à l'information et sur la protection des renseignements personnels sur une base régulière.

Ce registre comprend notamment :

- le descriptif de la demande;
- le système d'information analysé;

- les risques identifiés en matière de PRP et de sécurité de l'information;
- les mesures obligatoires identifiées en matière de PRP et de sécurité de l'information;
- la finalité de l'analyse.

Les mesures obligatoires identifiées au registre peuvent faire l'objet de suivis et vérifications auprès des personnes demanderesses par la personne RPRP-CSIO .

11 INVENTAIRE ET CLASSIFICATION DE L'ACTIF INFORMATIONNEL

Tout système d'information faisant l'objet d'une acquisition, une refonte ou une mise à jour doit être inscrit à l'inventaire des actifs informationnels de l'Université. Une personne détentrice de l'information membre du personnel cadre doit être désignée et la classification de l'information doit être réalisée ou révisée.

12 RESPONSABLE DE L'APPLICATION

Le Secrétariat général est responsable de l'application de cette directive.

13 MISE À JOUR

La présente directive est mise à jour tous les trois (3) ans, ou plus souvent si des modifications sont nécessaires.

14 ENTRÉE EN VIGUEUR

La présente directive entre en vigueur à compter de la date de son adoption.