Université de Sherbrooke

**DIRECTIVE 2600-093**

| | | | |
|---|---|---|---|
| **TITRE :** | **Directive de gestion des incidents de sécurité de l'information** | | |
| **ADOPTION :** | Comité de direction de l'Université | Résolution : | CD-2023-04-03-10 |
| **ENTRÉE EN VIGUEUR :** | 2023-04-03 | | |
| **MODIFICATION :** | Comité de direction de l'Université | Résolution : | |

## TABLE DES MATIÈRES

## PRÉAMBULE

L'Université de Sherbrooke doit protéger l'information, tout en tenant compte de sa valeur, afin d'en assurer la disponibilité, l'intégrité, et la confidentialité. Ces mesures de protection peuvent être préventives ou réactives. La présente directive assure une réaction cohérente et efficace lors d'un incident de la sécurité de l'information.

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) a permis au Conseil du trésor d'établir la *Directive gouvernementale sur la sécurité de l'information* (décret 1514-2021). Cette directive crée des obligations aux établissements universitaires en leur qualité d'organismes publics. Ainsi, l'Université de Sherbrooke a adopté sa *Politique de sécurité de l'information* (Politique 2500-036) et doit mettre en œuvre une *Directive de gestion des incidents de sécurité de l'information* (Directive 2600-093).

## 1 OBJECTIF

La présente directive définit une approche structurée de gestion des incidents de sécurité de l'information afin de repérer les incidents, de les gérer promptement, de limiter les différents impacts de chaque incident et de tirer des apprentissages de ces évènements.

## 2 CHAMP D'APPLICATION

Cette directive porte sur les actifs informationnels de l'Université :

- lui appartenant ou placés sous sa responsabilité, incluant, sans s'y limiter, le réseau informatique et de télécommunications;
- gérés directement par elle ou par un tiers;
- peu importe leur forme, leur média, leur technologie, leur langue, leur localisation et leur provenance;
- exploités directement ou indirectement afin d'utiliser des actifs informationnels d'un tiers.

Elle concerne tout membre de la communauté universitaire, quels que soient son rôle et son lieu, qui est tenu de la connaître et de s'y conformer. Cette responsabilité s'étend à tout fournisseur ou partenaire de l'Université, incluant les sous-traitants.

## 3 DÉFINITIONS[1]

**Actif informationnel** : une information, une banque d'information, un système ou un support d'information, un document, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par l'Université habituellement accessible ou utilisable avec un dispositif des technologies de l'information (logiciels, progiciels, didacticiels, banques de données et d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale). Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique dont le papier.

**Confidentialité :** Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

[1] Toutes les définitions proviennent de la *Politique de sécurité de l'information* (2500-036)

**Détentrice ou détenteur d'actif informationnel :** La personne membre du personnel cadre détenant la plus haute autorité au sein d'une unité académique ou administrative et dont le rôle consiste notamment, du point de vue décisionnel, fonctionnel ou opérationnel, à veiller à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous la responsabilité de cette unité. Aux fins de l'application de la présente Directive, il peut s'agir d'un autre membre du personnel-cadre de l'unité désigné par la personne qui détient la plus haute autorité au sein de l'unité.

**Disponibilité** : la propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

**Incident de sécurité de l'information** : un événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

**Intégrité** : Propriété d'une information de ne subir aucune altération ni destruction sans autorisation ou de façon erronée.

## 4 CADRE JURIDIQUE ET INSTITUTIONNEL

La *Directive de gestion des incidents de sécurité de l'information* est applicable en considérant les politiques et les directives suivantes applicables à l'Université de Sherbrooke :

- la *Politique de gestion intégrée des risques* (Politique 2500-031);
- la *Politique de sécurité de l'information* (Politique 2500-036);
- la *Directive relative à l'utilisation, à la gestion et à la sécurité des actifs informationnels* (Directive 2600-063);
- la *Procédure de gestion des incidents de confidentialité impliquant un renseignement personnel* (Procédure 2600-092);
- la *Loi sur la gouvernance des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03);
- la *Loi sur l'accès aux documents des organismes publics et à la protection des renseignements personnels* (RLRQ, c. A-2.1);
- la Directive gouvernementale sur la sécurité de l'information (décret numéro 1514-2021 du 8 décembre 2021);
- le *Cadre gouvernemental de gestion de la sécurité de l'information*
- le *Processus de gestion de menaces, des vulnérabilités et des incidents* du Centre gouvernemental de cyberdéfense.

## 5 PRINCIPES

L'Université doit fournir une assurance raisonnable que les incidents de sécurité de l'information sont adéquatement enregistrés, analysés et résolus selon un processus formel. À cette fin, une procédure de gestion des incidents doit être mise en place et tenir compte des exigences de sécurité applicables aux environnements technologiques de l'Université. Les principes suivants supportent le processus de gestion des incidents de sécurité de l'information. Par ailleurs, un incident de sécurité de l'information peut aussi comporter un incident de confidentialité impliquant un renseignement personnel. La présente directive est ainsi étroitement associée à la *Procédure de gestion des incidents de confidentialité impliquant un renseignement personnel* (Procédure 2600-092). Cette procédure précise les démarches à effectuer lorsque l'Université a des motifs raisonnables de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient ou si un tel incident est avéré, et ce, conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* RLRQ, c. A-2.1.

### 5.1 Préparer

#### 5.1.1 Formation et sensibilisation

Les concepts clés ainsi que les aspects spécifiques du plan de gestion des incidents doivent être incorporés au programme de formation et de sensibilisation de l'Université.

#### 5.1.2 Registre des incidents

Tous les incidents doivent être documentés dans le Registre des incidents de sécurité.

Les éléments suivants doivent minimalement être documentés tout au long de l'incident :

- Chronologie des évènements
- Dates et heures de chaque évènement pertinent
- Description sommaire des évènements
- Identification des actifs informationnels et indicateurs de compromission associés aux évènements
- Collecte des informations en lien avec la réponse telles que le signalement, les actions entreprises, les impacts et les résultats des analyses.

#### 5.1.3 Plan de communication

L'Université doit établir des plans de communications internes et externes en fonction de la sévérité des incidents décrite dans le procédurier de gestion des incidents.

#### 5.1.4 Utilisation de services externes

L'Université peut faire appel à des services externes pour compléter ou rehausser sa capacité à protéger ses actifs informationnels.

Spécifiquement, l'Université peut mandater un ou plusieurs prestataires de services pour effectuer les services suivants :

- Surveillance d'évènements de sécurité
- Vigie des menaces
- Assistance à la réponse aux incidents
- Simulation d'incidents
- Autres services complémentaires

Dans le cas où des prestataires externes sont impliqués, les rôles et responsabilités, les modalités d'intervention, les points de contact, l'entente de confidentialité, les niveaux de service et les procédures d'escalade doivent être clairement documentés. Il est de la responsabilité de la Cheffe ou du Chef de la sécurité de l'information organisationnelle (CSIO) et de la Coordonnatrice organisationnelle ou du coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) de communiquer les informations liées à l'incident de manière sécuritaire et efficace.

#### 5.1.5 Simulation d'incidents

Afin de valider l'efficacité du plan de réponse aux incidents, l'Université doit procéder à des exercices périodiques de simulation d'incidents. Ces exercices permettent de s'assurer que les divers intervenants comprennent leurs responsabilités respectives et connaissent les actions à prendre ainsi que la séquence dans laquelle elles doivent être posées.

#### 5.1.6 Prévention des incidents

L'Université doit s'assurer que des contacts appropriés sont entretenus avec les autorités, les groupes d'intérêt externes et les forums qui traitent des questions relatives aux incidents liés à la sécurité de l'information.

### 5.1.7 Procédure de gestion des incidents

Afin de maximiser l'efficacité des activités effectuées lors de l'occurrence d'un incident de sécurité de l'information, l'Université doit se doter d'une procédure de gestion des incidents de sécurité. Celle-ci permet de préparer l'institution à répondre adéquatement et à structurer la démarche à ce sujet.

La procédure de gestion des incidents de sécurité de l'information doit minimalement couvrir les aspects suivants :

- Enregistrement de l'incident de cybersécurité
- Prise de contact avec les personnes concernées par l'incident
- Analyse et triage de l'incident, incluant l'analyse d'un incident de confidentialité, le cas échéant
- Confinement, éradication et rétablissement
- Planification et mise en œuvre des actions correctives pour empêcher les récurrences
- Signalement de l'action à l'autorité compétente
- Bilan de l'incident

### 5.1.8 Obligation de signalement

Les utilisatrices et les utilisateurs doivent être informés de leur obligation de signaler tout incident lié à la sécurité de l'information dans les meilleurs délais. Ils doivent être informés de l'existence d'une procédure de signalement des évènements liés à la sécurité de l'information ainsi que de la *Procédure de gestion des incidents de confidentialité impliquant un renseignement personnel* (Procédure 2600-092).

Les utilisatrices et les utilisateurs sont informés de leurs obligations de déclarer tout évènement de sécurité de l'information (par exemple, le non-respect des directives mises en place, un dysfonctionnement logiciel ou matériel, une vulnérabilité, etc.).

Les évènements sont signalés dès que possible en utilisant les canaux validés par l'Université de Sherbrooke.

## 5.2 Détecter, analyser, informer

### 5.2.1 Détection et signalement des incidents

L'Université doit mettre en place les mécanismes de surveillance permettant d'identifier les évènements associés à des incidents de cybersécurité.

À cette fin, une procédure et des outils de surveillance des systèmes doivent être mis en place afin de prévenir et détecter les incidents.

La surveillance ainsi que le registre des incidents doivent permettre d'identifier les incidents récurrents pour fins d'amélioration continue.

Des moyens de communication et des processus de signalement permettant aux utilisatrices et aux utilisateurs de déclarer les évènements et incidents de la sécurité de l'information sont en place à l'Université de Sherbrooke.

Dès le début de la phase de détection et d'analyse, la ou le COMSI doit informer la personne responsable de la protection des renseignements personnels (RPRP) s'il y a un doute que des renseignements personnels soient en cause dans l'incident.

### 5.2.2 Mesures de réponses immédiates

Afin de limiter les impacts de l'incident et de préserver les traces, des mesures d'urgence peuvent être prises par la ou le COMSI à la suite de la première analyse sans approbation préalable. Le cas échéant, il doit en informer la ou le CSIO sans délai.

Tout actif informationnel faisant l'objet d'un incident de sécurité de l'information est isolé totalement, ou partiellement sur recommandation du COMSI, du reste du système d'information de l'Université de Sherbrooke.

### 5.2.3 Traitement

La ou le COMSI, après la phase d'évaluation de préjudice initial et de priorisation, effectue une évaluation de la nature de l'incident permettant une revue de la priorité des incidents.

En complément des mesures de réponses immédiates déjà prises dès la qualification de l'incident, des mesures complémentaires viendront prévenir toute aggravation de la situation ou arrêter l'incident.

Disposant à ce stade des informations obtenues lors des investigations, ces mesures seront davantage ciblées que les réponses conservatoires d'urgence :

- Restriction temporaire d'accès aux réseaux et aux applications;
- Communications ciblées;
- Reconstruction et remise en fonction des services interrompus.

Dès les phases initiales de l'occurrence de l'incident de sécurité de l'information, l'ensemble des actions relatives au traitement de l'incident est enregistré dans le registre des incidents de sécurité de l'information tenu par la ou le COMSI.

### 5.2.4 Collecte et conservation des preuves

Un processus de collecte et de conservation de preuves est formalisé et appliqué. Ce processus consiste à récupérer et à stocker toutes les informations pertinentes qui peuvent aider à identifier la source de l'incident, la portée des dommages causés et à établir la responsabilité. Cela peut inclure des données telles que des journaux système, des captures d'écran, des fichiers, des copies de disque et des espaces de stockage physique, virtuel ou infonuagique.

### 5.2.5 Incidents à portée gouvernementale

Un incident est qualifié à portée gouvernementale en présence d'un évènement de sécurité de l'information qui affecte l'image du gouvernement, dans son ensemble, et la confiance des citoyennes et des citoyens en termes de disponibilité, d'intégrité et de confidentialité d'un actif informationnel. Plus précisément, l'évènement sera caractérisé par une ou plusieurs des caractéristiques suivantes :

- Avoir un impact sur plus d'un organisme public
- Affecte des services indispensables à la population (besoins élémentaires, psychologiques)
- Met en danger la santé ou le bien-être d'un groupe d'individus

## 5.3 Confiner, éradiquer, rétablir

### 5.3.1 Remédiation des incidents

La détentrice ou le détenteur de l'actif informationnel doit s'assurer que des procédures de remédiation permettant d'assurer un traitement et une résolution adéquate des incidents impactant leurs actifs soient en place, et ce, dans les temps appropriés.

La détentrice ou le détenteur doit attester de l'adéquation des correctifs ou des mesures de mitigation mises en place en fonction du niveau de criticité des actifs informationnels et des normes en vigueur.

### 5.4 Apprendre

#### 5.4.1 Bilan de l'incident

L'Université de Sherbrooke doit procéder à une investigation post-incident afin de comprendre ce qui s'est produit et comment empêcher de futures occurrences. L'objectif de cette phase est de déterminer la cause de l'incident, d'évaluer les dommages causés, d'identifier les responsabilités et de recommander des mesures pour renforcer la sécurité informatique.

## 6 RÔLES ET RESPONSABILITÉS

### 6.1 Parties prenantes de la cellule de crise opérationnelle

#### 6.1.1 Cheffe ou Chef de la sécurité de l'information organisationnelle (CSIO)

La ou le CSIO est le propriétaire du processus de gestion des incidents en sécurité de l'information. Il est responsable de l'efficacité de la gestion des incidents et de l'exécution efficace et précise du processus. Il a comme responsabilités :

- Coordonner la cellule opérationnelle de crise
- Conserver à jour un plan d'action par rapport aux incidents majeurs et critiques de sécurité de l'information dans la valise de garde
- Approuver et présenter le rapport final aux instances

#### 6.1.2 Coordonnatrice organisationnelle ou coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

- Déterminer le niveau d'impact des préjudices
- Coordonner la gestion de l'incident sur le plan opérationnel
- Assurer le lien avec le COCD (Centre opérationnel de cyberdéfense) durant l'incident
- Soutenir l'équipe de sécurité informatique
- Saisir le responsable de la protection des renseignements personnels, dès que des renseignements personnels sont touchés par l'incident.

#### 6.1.3 Direction générale des services commerciaux et des assurances

- Colliger l'information nécessaire
- Contacter les assureurs, dont le cyberassureur
- Relayer l'information obtenue au CSIO et au COMSI
- Comptabiliser les coûts excédants relatifs aux ressources humaines et aux équipes externes

#### 6.1.4 Direction générale du service des communications

- Préparer le plan de communication interne et externe
- Coordonner les communications vers la communauté universitaire et l'externe
- Prévoir les modalités de communication en situation de crise, autre que le courriel

#### 6.1.5 Direction générale du service de la mobilité, de la sécurité et de la prévention (SMSP)

- Déterminer les impacts sur les personnes
- Activer les mesures d'urgence, le cas échéant
- Convoquer le CCPMU, le cas échéant

#### 6.1.6 Direction de l'Université (au besoin)

- Approuver le plan d'action recommandé par la cellule de crise opérationnelle
- Approuver les communications institutionnelles et externes
- Informer le président du CA de l'état de la situation

### 6.2 Comités

#### 6.2.1 Équipe tactique du Service des technologies de l'information (STI)

##### 6.2.1.1 Composition

- Coordonnatrice organisationnelle ou coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)
- Analyste en sécurité informatique
- Technicienne ou technicien en sécurité informatique
- Au besoin, d'autres personnes peuvent être invitées à participer

##### 6.2.1.2 Responsabilités

- Prendre en charge l'incident avec diligence avec les principaux intervenants dans les facultés et services
- Surveiller l'évolution de la situation
- Tenir informé la ou le CSIO
- Identifier les indices de compromission et établir la sévérité de l'incident
- Déterminer s'il existe un outil de remédiation
- Établir le plan d'action pour confiner, éradiquer et récupérer
- Ajuster les règles de détection et de filtrage
- Vérifier le plan de rétablissement

#### 6.2.2 Cellule de crise opérationnelle

##### 6.2.2.1 Composition

- Rectrice adjointe ou recteur adjoint
- Cheffe ou Chef de la sécurité de l'information organisationnelle (CSIO), qui préside
- Secrétaire générale ou secrétaire général
- Vice-rectrice ou vice-recteur de qui relève le STI
- Direction générale du STI
- Direction générale du Service de la mobilité, de la sécurité et de la prévention (SMSP)
- Direction générale du Service des communications
- Direction des Services commerciaux et des assurances
- Conseillère ou conseiller en sécurité de l'information
- Au besoin, d'autres personnes peuvent être invitées à participer à la cellule notamment les détenteurs d'actifs informationnels

##### 6.2.2.2 Responsabilités

- Évaluer l'impact de l'incident au niveau organisationnel en fonction de l'analyse de préjudice et du risque
- Déterminer le besoin de recourir à des ressources expertes externes
- Déterminer le besoin de convoquer le comité de coordination pour les mesures d'urgence (CCPMU)
- Réévaluer périodiquement la situation et convenir des suivis à court terme pour suivre l'évolution de l'incident
- Tenir informé le comité de direction de l'Université
- Recommander un plan d'action au comité de direction selon la gravité et le niveau de risque de l'incident.

#### 6.2.3 Comité de coordination pour les mesures d'urgence (CCPMU)

Le comité de coordination agit à l'intérieur de son mandat tel que défini dans le Plan des mesures d'urgence. Ce plan organise les mesures intégrées et cohérentes afin d'assurer la protection des personnes et des biens en cas de situation d'exception.

### 6.3 Conseil d'administration de l'Université

Le conseil d'administration est informé de changements importants à la situation à la suite d'un incident de sécurité de l'information selon le niveau de risque. Il prend toute décision utile à la demande de la rectrice ou du recteur.

## 7 SANCTION

Toute contravention à la présente directive est susceptible de sanctions conformément aux dispositions de la *Politique de sécurité de l'information* (Politique 2500-036).

## 8 RESPONSABILITÉ

La secrétaire générale ou le secrétaire général est responsable de la diffusion et de la mise à jour de la présente directive.

## 9 ENTRÉE EN VIGUEUR

La présente directive est entrée en vigueur à la date de son adoption par le comité de direction de l'Université, le 3 avril 2023.