Politique de Sécurité des Systèmes d'Information (PSSI)

1 OBJET DU PRESENT DOCUMENT

HYDRO Exploitation SA accorde une importance essentielle à la protection de ses informations, de ses systèmes et des données qui lui sont confiées.

La présente Politique de Sécurité de l'Information définit les engagements et principes directeurs en matière de sécurité de l'information. Elle a pour objectif d'assurer la confidentialité, l'intégrité et la disponibilité des informations, de soutenir la continuité des activités, de respecter les exigences applicables et de préserver la confiance des collaborateurs, clients, partenaires et autres parties prenantes. Cette politique constitue le cadre général de référence en matière de sécurité de l'information. Elle est complétée, lorsque cela est nécessaire, par des règles internes, directives et procédures précisant ses modalités d'application. Le présent document constitue une version publique synthétique de la politique en vigueur au sein de l'entreprise, dont les dispositions détaillées sont définies dans les documents internes.

2 CHAMP D'APPLICATION

La présente politique s'applique à l'ensemble des activités relevant du système d'information ainsi qu'à toute personne ayant accès, de manière autorisée, aux informations ou aux systèmes. Elle concerne les collaborateurs, partenaires, prestataires et tiers autorisés. Elle couvre l'ensemble des informations, quels que soient leur support, leur format, leur mode de traitement ou leur lieu de conservation. Le périmètre détaillé du système de management de la sécurité de l'information est défini dans les documents internes.

3 ENGAGEMENT DE LA DIRECTION

La Direction reconnaît que la sécurité de l'information constitue un enjeu stratégique majeur.
Elle s'engage à définir, soutenir, maintenir et améliorer un dispositif de sécurité adapté aux risques et cohérent avec les besoins de l'organisation. Cet engagement vise à protéger les actifs informationnels, garantir un niveau de sécurité approprié, respecter les obligations légales, réglementaires et contractuelles applicables, notamment en matière de protection des données, et assurer la continuité des activités et des services essentiels. Elle veille à mettre à disposition les ressources nécessaires et à promouvoir une culture de sécurité partagée. La gouvernance de la sécurité de l'information est structurée. Les rôles, responsabilités et autorités sont définis, attribués et régulièrement revus afin d'assurer une gestion cohérente et efficace du dispositif.

4 PRINCIPES DIRECTEURS

La sécurité de l'information repose sur des principes clairs qui guident l'ensemble des actions de protection et orientent l'organisation des mesures de sécurité.

Toutes les activités s'inscrivent dans un cadre de conformité. L'organisation veille au respect des exigences légales, réglementaires, contractuelles et normatives applicables et s'appuie sur des bonnes pratiques reconnues, notamment issues de la norme ISO/IEC 27001 et de référentiels associés.

La sécurité est fondée sur une approche systématique des risques. Les menaces susceptibles d'affecter les informations, les systèmes et les infrastructures sont identifiées, évaluées et traitées de manière proportionnée.

Elle repose également sur une culture de sécurité partagée, intégrée dans les activités quotidiennes et soutenue par des comportements responsables et une vigilance collective.

La sensibilisation, l'information et la formation régulières permettent à chaque personne concernée de comprendre son rôle et ses responsabilités. Le respect des règles internes constitue un élément essentiel de la maîtrise des risques et de la résilience.

Les exigences de sécurité sont intégrées dès la conception des processus, des projets, des systèmes et des services, puis tout au long de leur cycle de vie.

Tout événement susceptible d'affecter la sécurité de l'information est détecté, signalé et traité de manière structurée afin d'en limiter les impacts et de renforcer durablement le niveau de protection.

La continuité des activités est assurée par des mesures adaptées permettant de maintenir ou de rétablir les services essentiels dans des délais appropriés.

Enfin, la sécurité de l'information s'inscrit dans une démarche d'amélioration continue, fondée sur les retours d'expérience, les résultats de surveillance, les audits et l'évolution du contexte et des menaces.

5 CADRE DOCUMENTAIRE

La présente politique constitue le niveau stratégique du dispositif de sécurité de l'information. Elle est déclinée au travers d'un ensemble cohérent de documents internes qui en assurent la mise en œuvre opérationnelle. Ces documents définissent les règles applicables, les modalités pratiques et les mesures de sécurité nécessaires à la protection des informations. Cette organisation repose sur une structuration en plusieurs niveaux complémentaires, permettant d'assurer la cohérence entre les orientations stratégiques et leur application concrète. Les règles ainsi définies s'imposent à toute personne concernée.

6 MISE EN OEUVRE

La politique constitue le cadre général de la sécurité de l'information. Sa mise en œuvre repose sur des dispositions internes adaptées aux activités. Celles-ci précisent les règles applicables, les comportements attendus et les mesures de protection à respecter. Toute personne concernée contribue, à son niveau, à la protection des informations et des systèmes.

7 COMMUNICATION ET ENGAGEMENT

La présente politique est portée à la connaissance des personnes concernées par les moyens appropriés et peut être communiquée en interne comme en externe. Toute personne relevant de son champ d'application reconnaît en avoir pris connaissance et s'engage à respecter les principes et règles qui en découlent dans le cadre de ses activités.

Pour la Direction

Sion, le 27.04.2026

Matthias GAUMANN (27 avr. 2026 11:47:07 GMT+2)

Arnaud SCHALLER (27 avr. 2026 11:42:12 GMT+2)