MESURES DE SÉCURITÉ

Section 6 de ISO 27002:2022

Applicables à la section 6 de la norme ISO 27002:2022

Objectifs de la suite de documents

- Encadrer le cycle de vie des employés
- Réduire les risques humains et les erreurs
- Aider dans le processus pour obtenir une certification ISO 27001 et autres

Contexte des documents

Documents utilisant ISO 27002:2022 pour vous aider dans l'amélioration de vos pratiques en sécurité de l'information

Gestion du facteur humain

De l'embauche à la fin d'emploi : sécuriser chaque étape

Vue d'ensemble des contrôles 6.1 à 6.8

Mesures de sécurité liées aux personnes (ISO/IEC 27002:2022)

Chapitre 6

6.1 Présélection

Vérifier les antécédents de tous les candidats avant l'embauche, proportionnellement au niveau de risque et aux lois applicables.

6.2 Termes et conditions de contrat

Les contrats de travail doivent stipuler les responsabilités en matière de sécurité de l'information pour les utilisateurs de l'organisation.

6.3 Sensibilisation, enseignement et formation en sécurité de l'information

Les employés doivent recevoir une formation appropriée et des mises à jour régulières sur la sécurité de l'information.

6.4 Processus disciplinaire

Un processus formel doit être en place pour sanctionner les violations des politiques et directives de sécurité de l'information.

6.5 Responsabilités à la fin ou à la modification du contrat de travail

Protéger les intérêts de l'organisation lors d'un changement de poste ou d'un départ (restitution d'actifs, révocation d'accès, etc.).

6.6 Accords de confidentialité ou de non-divulgation (NDA)

Les employés et parties externes doivent signer des accords de confidentialité reflétant les besoins de protection de l'information.

6.7 Travail à distance (télétravail)

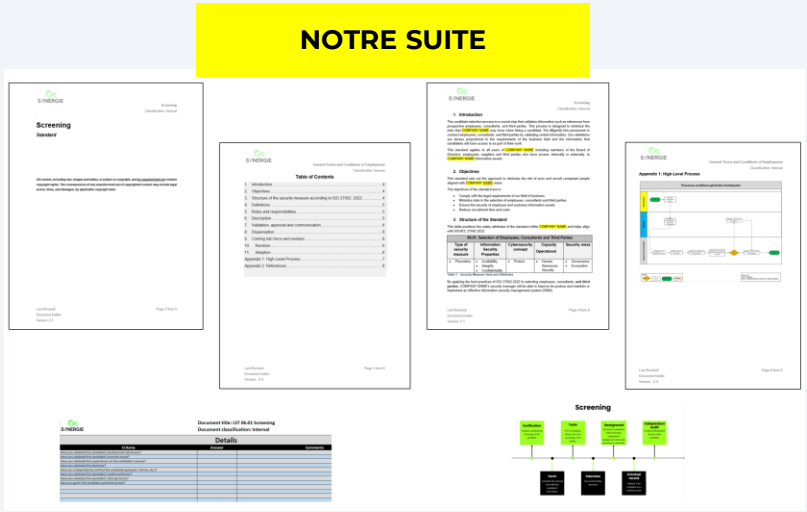
Des mesures de sécurité doivent être mises en œuvre pour protéger les informations lors du travail à distance ou à distance.

6.8 Signalement des événements liés à la sécurité de l'information

Les employés doivent signaler les événements de sécurité suspects via des canaux appropriés et le plus rapidement possible.

GAIN DE TEMPS

NOTRE SUITE



Série de documents section 6

8 Standards • 6 Processus • 3 Formulaires

Prêt à être utilisé

Série de documents - Contrôles liés aux personnes

Ne réinventez pas la roue : accélérez votre conformité et améliorez vos pratiques rapidement

La conformité ne devrait pas signifier des centaines d'heures de rédaction. Obtenez des documents structurés, préparés par des experts et prêts à l'emploi pour sécuriser votre capital humain immédiatement.

Documents structurés

Standards et procédures alignés sur les exigences ISO.

Implantation rapide

Modèles pré-remplis et personnalisables pour un déploiement en quelques minutes.

Sécurité renforcée

Réduisez le risque humain et uniformisez vos pratiques RH sans trop d'effort.

Communiquez avec nous →

Ce qui est inclus dans la suite

Une suite complète de documents prêts à l'emploi

Standards

8 Directives

- Sensibilisation & formation
- Télétravail (sécurité mobile)
- NDA / Confidentialité
- Conditions d'emploi
- Mesures disciplinaires
- Responsabilités post-emploi
- Vérifications (Screening)
- Signalement d'événements

Processus

6 Processus

- Recrutement et vérifications
- Arrivé (accès & SI)
- Gestion des manquements
- Changement de poste
- Départs
- Signalement et triage

Outils RH

3 Formulaires + 1 Lettre

- Attestation de formation
- Accord de confidentialité
- Demande d'autorisation

- Lettre de responsabilités post-emploi (modèle)

Sensibilisation

1 Support PPT

- Support de sensibilisation du personnel

Accélérez votre conformité dès aujourd'hui

Communiquez avec nous

RENFORCER LA SÉCURITÉ LIÉE AUX PERSONNES

Conclusion et perspectives pour la conformité

Réduction du risque

Diminuez significativement les risques d'erreurs humaines et de menaces internes grâce à un encadrement rigoureux du cycle de vie des données, accès, etc..

Conformité & audit

Assurez une conformité continue aux exigences de l'ISO avec des processus documentés.

Culture de sécurité

Développez une forte culture de sécurité où chaque employé est sensibilisé, formé et responsabilisé dès son arrivée.

PROCHAINES ÉTAPES RECOMMANDÉES

1. **Évaluer la maturité actuelle (GAP Analysis)**
2. **Déployer des politiques et contrôles RH**
3. **Former et sensibiliser le personnel**
4. **Mesurer l'efficacité avec mon aide.**

Annexe – Infographie section 6

6.1.png

6.2.png

6.3.png

6.4.png

6.5.png

6.6.png

6.7.png

6.8.png

ISO/IEC 27002:2022

Domaine 6 : Mesures liées aux personnes

CONTRÔLE CLÉ 🔑

6.1. Présélection (Screening)

Établir l'approche pour minimiser les risques d'erreur et recruter des personnes compétentes alignées sur la vision de l'entreprise.

Description de la mesure

Le processus de sélection des candidats permet de valider des informations comme les références des futurs employés, consultants et tiers visant à minimiser les risques que l'entreprise pourrait courir en engageant un candidat.

Objectifs

Conformité

Respecter les exigences légales de notre domaine d'affaires.

Évaluation des risques

Minimiser les risques dans la sélection des employés, consultants et tiers.

Processus formel

Le processus doit être documenté et appliqué de manière cohérente pour garantir l'équité et l'efficacité. De plus, le processus réduira le temps et les coûts de recrutement.

Attributs de la mesure 6.1

TYPE DE MESURE	PROPRIÉTÉS SÉCURITÉ DE L'INFORMATION	CONCEPT DE CYBERSÉCURITÉ	CAPACITÉ OPÉRATIONNELLE	DOMAINES DE SÉCURITÉ
• Préventive	• Disponibilité • Intégrité • Confidentialité	• Protéger	• Sécurité des ressources humaines	• Gouvernance • Écosystème

Tableau 1 - Vue de la mesure de sécurité et attributs (ISO 27002:2022)

Ceci est une représentation visuelle de la mesure 6.1 de l'ISO 27002:2022.
Ressource : https://synergieconsultation.com/produits/

ISO/IEC 27002:2022

Domaine 6 : Mesures liées aux personnes

CONTRÔLE CLÉ 🔑

6.2. Termes et conditions de contrat

Établir un ensemble de conditions d'emploi qui inclut la gestion de la sécurité de l'information.

Description de la mesure

Les termes et conditions d'emploi, ainsi que les contrats ou ententes conclus avec les employés et les consultants, doivent respecter les lois et normes en vigueur. Ils précisent clairement les responsabilités de chaque partie en matière de sécurité de l'information, y compris les obligations de confidentialité, les politiques applicables et les attentes spécifiques envers les utilisateurs de l'entreprise.

Par ces engagements contractuels, l'entreprise veille à renforcer la sensibilisation de son personnel et de ses partenaires à la sécurité de l'information, favorisant ainsi une culture organisationnelle responsable et conforme.

Objectifs

Clarification des rôles

Préciser et clarifier les rôles et les responsabilités en matière de sécurité de l'information dans les contrats d'embauche et d'ententes avec les employés et consultants.

Protection légale

Aider à respecter les exigences légales de notre domaine d'affaires.

Attributs de la mesure 6.2

TYPE DE MESURE	PROPRIÉTÉS SÉCURITÉ DE L'INFORMATION	CONCEPT DE CYBERSÉCURITÉ	CAPACITÉ OPÉRATIONNELLE	DOMAINES DE SÉCURITÉ
• Préventive	• Disponibilité • Intégrité • Confidentialité	• Protéger	• Sécurité des ressources humaines	• Gouvernance • Écosystème

Tableau 1 - Vue de la mesure de sécurité et attributs (ISO 27002:2022)

Ceci est une représentation visuelle de la mesure 6.2 de l'ISO 27002:2022.
Ressource : https://synergieconsultation.com/produits/

ISO/IEC 27002:2022

Domaine 6 : Mesures liées aux personnes

CONTRÔLE CLÉ 🔑

6.3 Sensibilisation, enseignement et formation en sécurité de l'information

Assurer que tous les utilisateurs reçoivent une formation adéquate en sécurité de l'information et qu'ils soient conscients de leurs responsabilités.

Description de la mesure

Assurer que tous les employés et consultants de l'entreprise reçoivent une formation appropriée, continue et adaptée à leurs fonctions en matière de sécurité de l'information.

Un programme structuré de sensibilisation à la sécurité permet d'outiller les utilisateurs, de renforcer leur vigilance et de favoriser une culture organisationnelle proactive où chacun comprend son rôle dans la protection de l'information et la résilience de l'entreprise.

Objectifs

Consolidation des acquis

Consolider et améliorer les connaissances et les acquis en sécurité de l'information des utilisateurs par des formations continues et adaptées.

Soutien à la gouvernance

Appuyer et renforcer l'adhésion à la politique et au cadre de gestion en sécurité de l'information de l'entreprise.

Attributs de la mesure 6.3

TYPE DE MESURE DE SÉCURITÉ	PROPRIÉTÉS SÉCURITÉ DE L'INFORMATION	CONCEPT DE CYBERSÉCURITÉ	CAPACITÉ OPÉRATIONNELLE	DOMAINES DE SÉCURITÉ
• Préventive	• Disponibilité • Intégrité • Confidentialité	• Protéger	• Sécurité des ressources humaines	• Gouvernance • Écosystème

Tableau 1 - Vue de la mesure de sécurité et attributs (ISO 27002:2022)

Ceci est une représentation visuelle de la mesure 6.3 de l'ISO 27002:2022.
Ressource : https://synergieconsultation.com/produits/

ISO/IEC 27002:2022

Domaine 6 : Mesures liées aux personnes

CONTRÔLE CLÉ 🔑

6.4. Processus disciplinaire

Veiller à ce que les utilisateurs comprennent les conséquences du non-respect de la politique et des directives de sécurité de l'information.

Description de la mesure

Processus qui sert à exprimer les conséquences d'un non-respect des règles de sécurité de l'information et des mesures qui seront prises à l'encontre des utilisateurs fautifs. Avant d'appliquer le processus, l'entreprise doit démontrer les faits et justifier toute mesure disciplinaire.

Objectifs

L'objectif principal est de veiller à ce que les utilisateurs comprennent les conséquences du non-respect.

Maintenir la conformité et la sensibilisation

Assurer la compréhension des conséquences par tous les utilisateurs et renforcer l'adhésion aux politiques et directives de sécurité de l'information.

Traitement équitable et proportionné

Garantir que toutes les mesures disciplinaires sont justifiées, appliquées de manière équitable et proportionnelle à la gravité de la faute et aux valeurs de l'entreprise.

Attributs de la mesure 6.4

TYPE DE MESURE DE SÉCURITÉ	PROPRIÉTÉS SÉCURITÉ DE L'INFORMATION	CONCEPT DE CYBERSÉCURITÉ	CAPACITÉ OPÉRATIONNELLE	DOMAINES DE SÉCURITÉ
• Corrective • Préventive	• Disponibilité • Intégrité • Confidentialité	• Répondre • Protéger	• Sécurité des ressources humaines	• Gouvernance • Écosystème

Tableau 1 - Vue de la mesure de sécurité et attributs (ISO 27002:2022)

Ceci est une représentation visuelle de la mesure 6.4 de l'ISO 27002:2022.
Ressource : https://synergieconsultation.com/produits/

ISO/IEC 27002:2022

Domaine 6 : Mesures liées aux personnes

CONTRÔLE CLÉ 🔑

6.5. Responsabilités à la fin ou à la modification du contrat de travail

Définir et appliquer un processus pour le retour des actifs, données et la révocation des droits d'accès lors du départ ou du changement de poste de l'utilisateur.

Description de la mesure

Le processus de fin d'emploi ou de modification de contrat vise à protéger les actifs, les informations et les systèmes de l'entreprise. Il assure la révocation rapide des droits d'accès, la restitution de tous les actifs et la confirmation des obligations post-emploi.

Objectifs

Protéger les données et actifs informationnels durant toute la durée et même après la fin d'un emploi ou du mandat ou lors de changements de poste afin de limiter les risques d'une utilisation personnelle ou malveillante.

Gestion des accès et actifs

Assurer la désactivation immédiate des droits d'accès de l'utilisateur et le retour de tous les actifs de l'entreprise lors de la fin du contrat. Appliquer les règles du contrat pour les modifications de poste.

Conformité légale et contractuelle

Confirmer que les responsabilités légales et contractuelles de l'employé ou consultant (y compris les accords de non-divulgation) sont maintenues et appliquées après le changement ou la fin de l'emploi.

Attributs de la mesure 6.5

TYPE DE MESURE DE SÉCURITÉ	PROPRIÉTÉS SÉCURITÉ DE L'INFORMATION	CONCEPT DE CYBERSÉCURITÉ	CAPACITÉ OPÉRATIONNELLE	DOMAINES DE SÉCURITÉ
• Préventive	• Disponibilité • Intégrité • Confidentialité	• Protéger	• Sécurité des ressources humaines • Gestion des actifs	• Gouvernance • Écosystème

Tableau 1 - Vue de la mesure de sécurité et attributs (ISO 27002:2022)

Ceci est une représentation visuelle de la mesure 6.5 de l'ISO 27002:2022.
Ressource : https://synergieconsultation.com/produits/

ISO/IEC 27002:2022

Domaine 6 : Mesures liées aux personnes

CONTRÔLE CLÉ 🔑

6.6. Accords de confidentialité ou de non-divulgation (NDA)

S'assurer que les utilisateurs et les parties externes respectent la confidentialité des informations de l'organisation.

Description de la mesure

Un accord de confidentialité ou de non-divulgation (NDA) se définit comme étant un accord signé entre deux parties afin de protéger les parties tout en les informant de leur responsabilité de protéger, utiliser et diffuser les informations de manière responsable et autorisée.

Objectifs

Uniformiser la gestion des ententes de confidentialité afin d'assurer l'application des lois, des règlements et des règles internes que l'entreprise est assujettie et de protéger la confidentialité des informations accessibles par les utilisateurs.

Conformité et uniformisation

Harmoniser et formaliser la gestion des accords de confidentialité pour garantir le respect des lois, des règlements et des politiques internes applicables à l'organisation.

Protection de la confidentialité des informations

Définir clairement les informations considérées comme confidentielles et les responsabilités des parties pour leur protection, assurant une compréhension unanime des attentes.

Attributs de la mesure 6.6

TYPE DE MESURE DE SÉCURITÉ	PROPRIÉTÉS SÉCURITÉ DE L'INFORMATION	CONCEPT DE CYBERSÉCURITÉ	CAPACITÉ OPÉRATIONNELLE	DOMAINES DE SÉCURITÉ
• Préventive	• Confidentialité	• Protéger	• Sécurité des ressources humaines • Protection des informations • Relations fournisseurs	• Gouvernance • Écosystème

Tableau 1 - Vue de la mesure de sécurité et attributs (ISO 27002:2022)

Ceci est une représentation visuelle de la mesure 6.6 de l'ISO 27002:2022.
Ressource : https://synergieconsultation.com/produits/

ISO/IEC 27002:2022

Domaine 6 : Mesures liées aux personnes

CONTRÔLE CLÉ 🔑

6.7. Travail à distance (Télétravail)

S'assurer que les informations et les actifs de l'organisation sont protégés lorsque le personnel travaille à distance.

💻 Description de la mesure

Des mesures de sécurité doivent être mises en place pour protéger les informations accessibles, traitées ou stockées sur les sites de travail à distance. Ces mesures doivent s'appliquer aux équipements (ordinateurs, téléphones, etc.), aux logiciels et aux réseaux utilisés par le personnel en télétravail.

L'organisation doit définir et faire appliquer des politiques claires concernant l'environnement de travail à distance, la sécurité physique, l'utilisation des réseaux et la réponse aux incidents afin de maintenir un niveau de sécurité équivalent à celui du bureau.

Objectifs

Encadrer et limiter autant que possible les risques qu'amène le travail à distance et protéger les informations de l'entreprise lorsque les employés ou les tiers travaillent à l'extérieur de l'organisation.

📜 Encadrement et responsabilités

Établir des règles de sécurité uniformes pour les utilisateurs à distance et définir clairement les rôles, les droits et les obligations de l'organisation et du personnel en télétravail.

🔒 Protection et risques

Contribuer à protéger la disponibilité, l'intégrité et la confidentialité des données et encadrer les risques inhérents au travail à distance.

Attributs de la mesure 6.7

TYPE DE MESURE DE SÉCURITÉ	PROPRIÉTÉS SÉCURITÉ DE L'INFORMATION	CONCEPT DE CYBERSÉCURITÉ	CAPACITÉ OPÉRATIONNELLE	DOMAINES DE SÉCURITÉ
• **Préventive**	• Disponibilité • Intégrité • Confidentialité	• Protéger	• Gestion des actifs • Protection des informations • Sécurité physique • Sécurité système et réseau	• Protection

Tableau 1 - Vue de la mesure de sécurité et attributs (ISO 27002:2022)

Ceci est une représentation visuelle de la mesure 6.7 de l'ISO 27002:2022.
Ressource : https://synergieconsultation.com/produits/

ISO/IEC 27002:2022

Domaine 6 : Mesures liées aux personnes

CONTRÔLE CLÉ 🔑

6.8. Signalement des événements liés à la sécurité de l'information

S'assurer que les événements de sécurité de l'information sont signalés aussi rapidement que possible par le biais des canaux de gestion appropriés.

📢 Description de la mesure

Les organisations doivent mettre en place des procédures pour permettre au personnel et aux parties prenantes de signaler rapidement les événements de sécurité (potentiels ou avérés), les faiblesses et les observations liées aux services.

Le signalement doit être effectué par le biais de canaux officiels définis (par exemple, centre de service, courriel dédié) et doit inclure tous les détails nécessaires pour permettre une analyse et une réponse efficace.

Objectifs

Permettre aux utilisateurs de déclarer rapidement et facilement les événements de sécurité de l'information avérés ou potentiels via les processus et canaux de communication officiels de l'entreprise.

🚨 Canaux et procédures

Établir des procédures et des canaux de communication clairs et connus pour le signalement de tout événement ou faiblesse de sécurité.

⏳ Action et amélioration continue

Assurer une détection rapide pour une réponse appropriée, minimiser les dommages et permettre de tirer des leçons pour prévenir la récurrence des incidents.

Attributs de la mesure 6.8

TYPE DE MESURE DE SÉCURITÉ	PROPRIÉTÉS SÉCURITÉ DE L'INFORMATION	CONCEPT DE CYBERSÉCURITÉ	CAPACITÉ OPÉRATIONNELLE	DOMAINES DE SÉCURITÉ
• **Détective**	• Disponibilité • Intégrité • Confidentialité	• Détecter	• Gestion des événements de la sécurité de l'information	• Défense

Tableau 1 - Vue de la mesure de sécurité et attributs (ISO 27002:2022)

Ceci est une représentation visuelle de la mesure 6.8 de l'ISO 27002:2022.
Ressource : https://synergieconsultation.com/produits/