[ajout facultatif au titre]

Concept de crise TIC
École: [Nom]

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Personne | Adaptations effectuées / Remarques |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |
| Responsable: [Responsables] |  | Créateur/Créatrice: Auteur |
| Éditeur/Éditrice: [Éditeur] | Date de création: 18.11.2024 | Destinataires | À l’attention de: [Destinataires] |

Sommaire

[1 Introduction et objectif 4](#_Toc183443452)

[1.1 Objectif du concept de sécurité 4](#_Toc183443453)

[1.2 Champ d’application et domaine d’application 4](#_Toc183443454)

[1.3 Définition des termes importants 4](#_Toc183443455)

[Chapitre 1 - État des lieux 6](#_Toc183443456)

[2 Infrastructure 6](#_Toc183443457)

[2.1 Infrastructure réseau 6](#_Toc183443458)

[2.2 Composants réseau 6](#_Toc183443459)

[2.3 Terminaux 6](#_Toc183443460)

[3 Gestion des contrats 6](#_Toc183443461)

[4 Protection de l’infrastructure réseau 6](#_Toc183443462)

[4.1 Contrôle d’accès au réseau 6](#_Toc183443463)

[4.2 Segmentation et gestion des sous-réseaux 6](#_Toc183443464)

[4.3 Protection contre les attaques externes (pare-feu, IPS/IDS, etc.) 6](#_Toc183443465)

[5 Protection des composants du réseau 7](#_Toc183443466)

[5.1 Politiques de sécurité pour les serveurs 7](#_Toc183443467)

[5.2 Gestion des périphériques réseau 7](#_Toc183443468)

[5.3 Patch Management 7](#_Toc183443469)

[5.4 Sécurité physique 7](#_Toc183443470)

[6 Protection des terminaux\*\* 7](#_Toc183443471)

[6.1 Directives pour les terminaux 7](#_Toc183443472)

[6.2 Cryptage et logiciels de sécurité 7](#_Toc183443473)

[6.3 Gestion des appareils mobiles (MDM) 7](#_Toc183443474)

[6.4 Directives BYOD 7](#_Toc183443475)

[6.5 Exigences de sécurité pour les appareils appartenant à l’école 7](#_Toc183443476)

[6.6 Séparation des données privées et scolaires 7](#_Toc183443477)

[7 Gestion des données et sauvegardes 8](#_Toc183443478)

[7.1 Concept de sauvegarde 8](#_Toc183443479)

[7.2 Stockage et archivage des données 8](#_Toc183443480)

[7.3 Récupération en cas d’urgence 8](#_Toc183443481)

[Chapitre 2 - Organisation et crise 9](#_Toc183443482)

[8 Analyse et évaluation des risques 9](#_Toc183443483)

[8.1 Formes de risques pour la sécurité 9](#_Toc183443484)

[8.2 Analyse des points faibles 10](#_Toc183443485)

[9 Sensibilisation et formation 10](#_Toc183443486)

[9.1 Définition des responsabilités 10](#_Toc183443487)

[10 Audits et évaluations de sécurité 10](#_Toc183443488)

[11 Mesures à prendre pendant et après un incident 10](#_Toc183443489)

[11.1 Équipe d’intervention 10](#_Toc183443490)

[11.2 Aides internes 11](#_Toc183443491)

[11.3 Aides externes 11](#_Toc183443492)

[11.4 Besoin d’informations 11](#_Toc183443493)

[11.5 Ressources d’information 11](#_Toc183443494)

[12 Analyse de la situation et mesures d’urgence 11](#_Toc183443495)

[12.1 Identification des données concernées 11](#_Toc183443496)

[12.2 Définir des mesures d’urgence 11](#_Toc183443497)

[Chapitre 3 - Documentation et rapports 13](#_Toc183443498)

[12.3 Documentation sur le concept de sécurité TIC 13](#_Toc183443499)

[12.4 Mécanismes de reporting 13](#_Toc183443500)

[Chapitre 4 - Annexes 14](#_Toc183443501)

[13 Listes de contacts 14](#_Toc183443502)

[14 Documentations produits 14](#_Toc183443503)

[15 Rapports 14](#_Toc183443504)

[16 Membres de l’équipe d’intervention de crise 14](#_Toc183443505)

***Remarques préliminaires***

*Les mots de passe et autres informations confidentielles ne doivent pas être écrits dans ce document. Ce document devant être utilisé dans les processus de validation et lors des formations, nous recommandons de stocker ces données secrètes dans un gestionnaire de mots de passe ou un document de référence accessible aux personnes autorisées.*

*Certains des chapitres suivants ne sont peut-être pas pertinents pour votre institution, d’autres manquent. Nous vous invitons à adapter le document selon vos besoins.*

*Le modèle de concept de sécurité TIC est disponible sous forme de document ouvert au format Microsoft® Word à l’adresse* [*www.swisscom.com/campus.*](http://www.swisscom.com/campus) *Il peut être cité, utilisé et modifié sans réserve, à condition d’en mentionner l’auteur.*

# Introduction et objectif

Le présent document sert de description de l’état des lieux des différents éléments du réseau TIC de l’école. Cliquez ou tapez directement dans le document pour ajouter du texte. Il clarifie en outre les questions importantes concernant les stocks de données à risque, leur protection et les mesures à prendre en cas d’incident.

Le présent document sert de modèle aux écoles et doit être adapté à la situation et aux besoins spécifiques d’une école ou d’un groupe d’écoles.

## Objectif du concept de sécurité

Le présent concept aide les responsables d’une école à avoir accès, en cas d’incident, à des informations actuelles sur l’infrastructure réseau TIC, à classer et à délimiter rapidement le problème et à prendre les mesures d’urgence nécessaires. Il ne sert pas à décrire ou à conceptualiser les mesures de sécurité à prendre en amont – pour ces questions, un concept de sécurité est élaboré au moment de la mise en place de l’architecture du réseau TIC.

## Champ d’application et domaine d’application

Ce concept de crise TIC est valable dès son entrée en vigueur et s’applique en cas de crise (d’incident). Il sert de base à l’équipe d’intervention de l’école pour délimiter l’incident, identifier les parties du réseau concernées, adresser les points de contact impliqués et enfin définir les mesures d’urgence nécessaires.

## Définition des termes importants

Insérez ici les composants TIC pertinents dans votre école et les éventuelles unités organisationnelles qui pourraient être importantes en cas d’incident:

|  |  |  |
| --- | --- | --- |
| Terminologie | Explication | Remarques |
| SPOC IT | (=Single Point of Contact) Interlocuteur de la commune pour les questions TIC | Jean Exemple+41 58 123 12 12  |
| Salle des serveurs «Ancien bâtiment» | Salle des serveurs dans l’école «Meieli», 1er sous-sol, salle 123 | Accès par passe-partout |
|  |  |  |

Chapitre 1 - État des lieux

# Infrastructure

## Infrastructure réseau

Complétez ici une description de l’infrastructure réseau telle qu’elle est décrite dans le concept de sécurité ou dans le concept d’architecture TIC. Un plan de réseau peut également s’avérer utile.

## Composants réseau

Complétez ici les composants réseau centraux qui pourraient être affectés en cas d’incident. Il s’agit notamment de ces éléments: les routeurs, les passerelles réseau, les fonctionnalités réseau et les serveurs sont tous pertinents.

## Terminaux

Décrivez ici le type de terminaux et la manière dont ils sont connectés ou peuvent être intégrés dans l’architecture du réseau. Décrivez en particulier si et comment le BYOD (=Bring Your Own Device) peut être intégré dans le réseau.

# Gestion des contrats

Énumérez ici tous les contrats, y compris les fournisseurs qui gèrent ou sont responsables de parties ou de composants de votre réseau scolaire au moyen de prestations de service. Ajoutez également les contacts d’assistance des fournisseurs.

# Protection de l’infrastructure réseau

## Contrôle d’accès au réseau

Décrivez ici les instruments qui permettent l’accès – virtuel et physique – au réseau. Cela vous permet d’identifier rapidement les portes d’entrée possibles.

## Segmentation et gestion des sous-réseaux

Si l’architecture TIC connaît une segmentation en sous-réseaux dont les transitions impliquent des mesures de sécurité particulières, vous pouvez les décrire ici.

## Protection contre les attaques externes (pare-feu, IPS/IDS, etc.)

Indiquez ici les composants de sécurité internes ou externes au réseau qui sont utilisés. Notez également à cet endroit les éventuelles informations d’accès ou de contact.

# Protection des composants du réseau

## Politiques de sécurité pour les serveurs

Décrivez ici les politiques de sécurité en vigueur pour des infrastructures de serveurs spécifiques.

## Gestion des périphériques réseau

Décrivez ici comment certains périphériques réseau, tels que les routeurs ou les points d’accès WLAN, sont gérés. Indiquez également par qui les composants correspondants sont gérés.

## Patch Management

Si vous utilisez un Patch Management automatique, semi-automatique ou manuel, vous pouvez décrire ici le processus et les responsabilités.

## Sécurité physique

Formulez ici l’accès et l’autorisation d’accès aux composants centraux du réseau tels que les routeurs, les points d’accès WLAN, les serveurs, etc.

# Protection des terminaux\*\*

## Directives pour les terminaux

Décrivez les politiques d’accès aux terminaux en vigueur dans votre école.

## Cryptage et logiciels de sécurité

S’il existe un cryptage particulier pour le trafic au sein de l’école vers des services spécifiques en dehors de l’école, vous pouvez le compléter ici.

Si un logiciel de sécurité spécifique (pare-feu, filtre de contenu) est installé sur les équipements scolaires, décrivez ici son exécution, son degré de fonctionnement et son implémentation.

## Gestion des appareils mobiles (MDM)

Décrivez le produit, la propagation et les éventuelles spécificités de sécurité d’un système de gestion des appareils mobiles utilisé dans votre école.

## Directives BYOD

Indiquez si le BYOD est utilisé et si oui: comment les terminaux n’appartenant pas à l’école (ordinateurs portables, smartphones, etc.) peuvent accéder au réseau de l’école.

## Exigences de sécurité pour les appareils appartenant à l’école

S’il existe des directives spécifiques concernant les exigences de sécurité pour l’utilisation de terminaux appartenant à l’école (par ex. lecteur d’empreintes digitales, built-in camera, etc.), exécutez-les ici.

## Séparation des données privées et scolaires

Si vous utilisez un modèle qui permet aux élèves et aux enseignants de configurer des profils d’utilisation personnels et scolaires sur leur appareil, veuillez décrire l’utilisation de cette option.

# Gestion des données et sauvegardes

##  Concept de sauvegarde

Décrivez quelles données sont sauvegardées et de quelle manière. La fréquence, la localisation et l’accès à ces sauvegardes sont particulièrement importants.

##  Stockage et archivage des données

S’il devait y avoir d’autres sauvegardes (physiques, hors réseau, non automatisées) des données: Décrivez ici le processus et la procédure correspondants, y compris les personnes de contact et la disponibilité.

##  Récupération en cas d’urgence

Clarifier avec les services responsables comment accéder à un jeu de sauvegarde en cas d’incident, comment se déroulera une restauration et comment valider l’intégrité des données restaurées.

Chapitre 2 - Organisation et crise

# Analyse et évaluation des risques

## Formes de risques pour la sécurité

Formulez ici les risques potentiels pour la sécurité. Vous trouverez ci-dessous une sélection de risques:

|  |  |  |
| --- | --- | --- |
| Risque | Description | Appréciation (pertinent/non pertinent; élevé-moyen-faible) |
| Infractions à la protection des données  | Accès non autorisé aux données personnelles des élèves, du corps enseignant et du personnel administratif. |  |
| Cyberattaques  | Il s’agit notamment d’hameçonnage, des logiciels malveillants, des attaques par rançongiciel et d’autres formes de cyberattaques visant à infiltrer le réseau de l’école. |  |
| Perte de données  | Perte de données importantes en raison de défauts techniques, d’erreurs humaines ou de cyberattaques. |  |
| Sauvegarde des données insuffisante  | Absence ou insuffisance de procédures de sauvegarde qui ne permettent pas la récupération en cas de perte de données |  |
| Utilisation abusive des ressources TIC  | Utilisation des TIC scolaires pour des activités inappropriées ou illégales par les élèves ou le personnel. |  |
| Risques liés aux logiciels  | L’utilisation de logiciels obsolètes ou sans licence peut entraîner des failles de sécurité et des problèmes juridiques. |  |
| Panne matérielle  | Défaillance de systèmes ou d’équipements critiques pouvant entraîner des interruptions de l’enseignement ou de l’administration. |  |
| Sécurité du réseau insuffisante  | Protection insuffisante du réseau contre les accès non autorisés ou les abus. |  |
| Manque de formation des utilisateurs  | Le corps enseignant, les élèves et le personnel administratif ne sont pas suffisamment formés à une utilisation sûre et responsable des TIC. |  |
| Risques physiques pour la sécurité  | Protection insuffisante des équipements TIC contre le vol, le vandalisme ou les catastrophes naturelles. |  |
| Contenu en ligne inapproprié  | Accès à des documents potentiellement nuisibles ou inappropriés sur Internet |  |
| Risques de conformité  | Violations des exigences légales ou réglementaires en matière de protection et de sécurité des données. |  |
| Dépendance vis-à-vis de prestataires de service tiers  | Perturbations de services achetés à l’extérieur (comme les fournisseurs de services Internet, services cloud). |  |
| Problèmes d’interopérabilité  | Difficultés d’intégration de nouvelles technologies dans une structure TIC existante ou manque de compatibilité entre différents systèmes et applications. |  |
| Social Engineering  | Tactiques incitant le personnel ou les élèves à révéler des informations confidentielles. |  |
| Menaces internes  | Risques émanant de personnes au sein de l’organisation, qu’il s’agisse d’actes intentionnels ou d’imprudences. |  |

## Analyse des points faibles

Effectuez une analyse décrivant plus précisément les risques pertinents/élevés énumérés ci-dessus. Il convient d’aborder des dimensions telles que la gravité, la probabilité d’occurrence, le nombre de personnes concernées ou les risques financiers.

# Sensibilisation et formation

## Définition des responsabilités

Définissez pour l’école le poste responsable de la sensibilisation de tous les groupes cibles au sein de votre école. Ce rôle est chargé d’informer les groupes à intervalles réguliers sur les risques potentiels. Définissez les modalités et la fréquence de ces actions de sensibilisation et prévoyez, au cas par cas, un budget correspondant.

# Audits et évaluations de sécurité

Déterminez à quelle fréquence, selon quel mode et par qui un audit de sécurité doit être réalisé pour votre école. En tant qu’école, vous avez la possibilité de réaliser vous-même un tel audit, de le confier à vos fournisseurs TIC ou de le confier à un tiers spécialisé.

# Mesures à prendre pendant et après un incident

## Équipe d’intervention

Établissez – de manière analogue à l’équipe d’intervention en cas de crise – un groupe de personnes et de fonctions de taille raisonnable qui, en cas d’incident, coordonne les premières étapes (voir ci-dessous, [12.2 Définir les mesures d’urgence](#_Sofortmassnahmen_definieren)). Décrivez également à ce stade la fréquence et le mode de pratique de ce groupe.

Avant même d’activer l’équipe d’intervention, il convient de clarifier les principales responsabilités. Cela concerne notamment le rôle du responsable de l’équipe d’intervention, le rôle de la communication ou l’implication de la communauté. Clarifiez également les remplacements.

## Aides internes

Identifiez en interne (dans le cadre d’un exercice) d’autres personnes ayant les connaissances requises auxquelles vous pouvez faire appel pour rejoindre l’équipe d’intervention en cas d’incident.

## Aides externes

Il existe divers prestataires de services qui proposent ce que l’on appelle un CSIRT-as-a-Service. Pour ce faire, des informations telles que celles mentionnées dans ce document et d’autres sont échangées au préalable avec le fournisseur. Dans ce contexte, un audit est souvent réalisé pour vous aider à identifier les zones de risque et à y remédier.
Décrivez ici dans quels cas et de quelle manière il faut et il est possible d’accéder aux ressources CSIRT. Déterminez également qui fera office de SPOC en cas d’appel.

Il existe divers prestataires de service qui proposent une offre de réponse rapide. En cas d’incident, de tels prestataires mettent à votre disposition une équipe de spécialistes qui vous soutiennent de manière renommée dans la gestion de la crise. Clarifiez quelles tâches et responsabilités seront attribuées à quel endroit en cas de recours à une équipe de réaction rapide.

## Besoin d’informations

Accordez une grande attention à la tâche d’informer les services concernés et devant être impliqués avec l’urgence et la précision nécessaires. Décrivez ici les groupes d’intérêt potentiels et leurs besoins en informations.

## Ressources d’information

Identifier toutes les informations pertinentes dont vous pourriez avoir besoin en cas d’incident ou qui pourraient vous aider à gérer les tâches. Structurez les sources d’information de manière hiérarchique (commune, canton, Confédération) et thématique (processus, technique, communication, etc.).

# Analyse de la situation et mesures d’urgence

## Identification des données concernées

Dès que vous avez des indices ou des soupçons concernant un incident, essayez de délimiter le plus rapidement possible quelles données sont concernées par l’incident. Les informations consignées au chapitre 1 au chiffre 4.2 Segmentation et gestion des sous-réseaux permettent d’isoler les différents sous-réseaux concernés.

## Définir des mesures d’urgence

1. **Sauvegarder les données non concernées.** Si seules certaines parties des données sont concernées, sécurisez en plus l’accès aux autres données en ce qui concerne le danger survenu. Par exemple, déconnectez d’autres serveurs du réseau, bloquez les connexions des terminaux concernés ou changez les mots de passe, etc.
2. **Établir un rapport** sur l’incident avec l’équipe d’intervention. Vous devriez actualiser régulièrement ce rapport pendant la crise et le diffuser, si nécessaire, par les canaux d’information utiles. Vous vous assurez ainsi que tous les services impliqués disposent à tout moment des informations les plus récentes.
3. **Créer un concept d’information.** Déterminez qui a besoin de quelles informations et à quel moment. Ne sous-estimez pas cette tâche et affectez-lui suffisamment de ressources humaines. Veillez en outre à recourir à un canal d’information qui n’est pas concerné par l’incident et qui jouit néanmoins de la confiance des destinataires (par exemple, ne pas utiliser une adresse électronique privée, mais une adresse officielle pour l’envoi).
4. **Recours à une aide interne et externe.** Selon l’organisation de vos réseaux TIC, certaines informations sont situées à des endroits différents. Informez immédiatement les services par le biais d’un rapport. Les ressources mentionnées au chiffre 4 Protection de l’infrastructure réseau vous aideront à prendre les bonnes décisions en cas de crise.
5. **Directives et instructions de comportement.** Établissez des règles de conduite pour l’équipe d’intervention, les autorités scolaires, le corps enseignant, les élèves et éventuellement les parents/personnes détentrices de l’autorité parentale (si nécessaire). Ceux-ci doivent servir à délimiter le dommage et, le cas échéant, à identifier les preuves et les indications.

Chapitre 4 - Documentation et rapports

## Documentation sur le concept de sécurité TIC

Décrivez ici les différents processus de documentation, notamment:

1. Création et mise à jour du document
2. Fréquence de vérification des informations mentionnées ici (informations de contact, contrats, descriptions de produits, etc.)
3. Documentation en cas d’incident

## Mécanismes de reporting

Décrivez ici comment et sous quelle forme les données relatives au trafic, aux sites web consultés, aux protocoles de connexion, etc. doivent être collectées, analysées, stockées, archivées et utilisées.

1. Annexes

# Listes de contacts

# Documentations produits

# Rapports

# Membres de l’équipe d’intervention de crise