[Optionaler Titelzusatz]

ICT-Krisenkonzept
Schule: [Name]

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Person | Vorgenommene Anpassungen/Bemerkungen |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |
| Verantwortlich: [Verantwortlich] |  | Ersteller\*in: Autor\*in |
| Herausgeber\*in: [Herausgeber]. | Erstellung: 18.11.2024 | Geht an | z.K. an: [Empfänger] |

Inhalt

[1 Einführung und Zielsetzung 4](#_Toc182921786)

[1.1 Zweck des Sicherheitskonzepts 4](#_Toc182921787)

[1.2 Geltungsbereich und Anwendungsbereich 4](#_Toc182921788)

[1.3 Definition wichtiger Begriffe 4](#_Toc182921789)

[Kapitel 1 - Bestandesaufnahme 5](#_Toc182921790)

[2 Infrastruktur 5](#_Toc182921791)

[2.1 Netzwerk-Infrastruktur 5](#_Toc182921792)

[2.2 Netzwerk-Komponenten 5](#_Toc182921793)

[2.3 Endgeräte 5](#_Toc182921794)

[3 Vertragsmanagement 5](#_Toc182921795)

[4 Schutz der Netz-Infrastruktur 5](#_Toc182921796)

[4.1 Netzwerkzugangskontrolle 5](#_Toc182921797)

[4.2 Segmentierung und Verwaltung von Subnetzen 5](#_Toc182921798)

[4.3 Schutz gegen externe Angriffe (Firewalls, IPS/IDS etc.) 5](#_Toc182921799)

[5 Schutz der Netzwerk-Komponenten 5](#_Toc182921800)

[5.1 Sicherheitsrichtlinien für Server 5](#_Toc182921801)

[5.2 Verwaltung von Netzwerkgeräten 6](#_Toc182921802)

[5.3 Patch-Management 6](#_Toc182921803)

[5.4 Physische Sicherheit 6](#_Toc182921804)

[6 Schutz der Endgeräte\*\* 6](#_Toc182921805)

[6.1 Richtlinien für Endgeräte 6](#_Toc182921806)

[6.2 Verschlüsselung und Sicherheitssoftware 6](#_Toc182921807)

[6.3 Mobile Gerätemanagement (MDM) 6](#_Toc182921808)

[6.4 BYOD-Richtlinien 6](#_Toc182921809)

[6.5 Sicherheitsanforderungen für schuleigene Geräte 6](#_Toc182921810)

[6.6 Trennung privater und schulischer Daten 6](#_Toc182921811)

[7 Datenmanagement und Backups 7](#_Toc182921812)

[7.1 Backup-Konzept 7](#_Toc182921813)

[7.2 Speicherung und Archivierung von Daten 7](#_Toc182921814)

[7.3 Wiederherstellung im Notfall 7](#_Toc182921815)

[Kapitel 2 - Organisation und Krise 8](#_Toc182921816)

[8 Risikoanalyse und -bewertung 8](#_Toc182921817)

[8.1 Formen der Sicherheitsrisiken 8](#_Toc182921818)

[8.2 Schwachstellen-Analyse 9](#_Toc182921819)

[9 Sensibilisierung und Schulung 9](#_Toc182921820)

[9.1 Festlegung der Verantwortlichkeiten 9](#_Toc182921821)

[10 Sicherheitsaudits und -bewertungen 9](#_Toc182921822)

[11 Massnahmen während und nach einem Incident 9](#_Toc182921823)

[11.1 Interventions-Team 9](#_Toc182921824)

[11.2 Interne Hilfestellungen 10](#_Toc182921825)

[11.3 Externe Hilfestellungen 10](#_Toc182921826)

[11.4 Informations-Bedarf 10](#_Toc182921827)

[11.5 Informations-Ressourcen 10](#_Toc182921828)

[12 Situationsanalyse und Sofortmassnahmen 10](#_Toc182921829)

[12.1 Identifikation betroffener Daten 10](#_Toc182921830)

[12.2 Sofortmassnahmen definieren 10](#_Toc182921831)

[Kapitel 3 - Dokumentation und Reporting 12](#_Toc182921832)

[12.3 Dokumentation zum ICT-Sicherheitskonzept 12](#_Toc182921833)

[12.4 Reporting-Mechanismen 12](#_Toc182921834)

[Kapitel 4 - Anhänge 13](#_Toc182921835)

[13 Kontaktlisten 13](#_Toc182921836)

[14 Produkt-Dokumentationen 13](#_Toc182921837)

[15 Reportings 13](#_Toc182921838)

[16 Mitglieder des Kriseninterventions-Teams 13](#_Toc182921839)

***Vorbemerkungen***

*Passwörter und andere geheime Informationen sollten Sie nicht in diesem Dokument niederschreiben. Da dieses Dokument in Freigabeprozessen und bei Schulungen eingesetzt werden sollte, empfehlen wir, diese geheimen Daten in einem für Berechtigte zugänglichen Passwortmanager oder Referenzdokument zu speichern.*

*Einige der nachfolgenden Kapitel sind für Ihre Institution eventuell nicht relevant, andere fehlen. Wir laden Sie ein, das Dokument nach Ihren Bedürfnissen anzupassen.*

*Das Musterkonzept ICT-Sicherheit ist als offenes Dokument im Format Microsoft® Word verfügbar unter* [*https://www.swisscom.com/campus*](https://www.swisscom.com/campus)*. Es darf unter Angabe der Urheberschaft ohne Vorbehalte zitiert, genutzt und verändert werden.*

# Einführung und Zielsetzung

Das vorliegende Dokument dient als Bestands-Beschrieb der unterschiedlichen ICT-Netzwerk-Elemente der Schule. Klicken oder tippen Sie direkt ins Dokument, um Text zu ergänzen. Zudem klärt es wichtige Fragen hinsichtlich risikobehafteter Datenbestände, deren Schutz sowie Massnahmen im Falle eines Incidents.

Das vorliegende Dokument dient als Blaupause für Schulen und soll auf die jeweilige Situation und den jeweiligen Bedarf einer Schule oder eines Schulverbunds angepasst werden.

## Zweck des Sicherheitskonzepts

Das vorliegende Konzept hilft den Verantwortlichen an einer Schule, im Falle eines Incidents auf aktuelle Informationen zur ICT Netzwerk-Infrastruktur zugreifen zu können, das Problem rasch einordnen und eingrenzen zu können und die nötigen Sofortmassnahmen einzuleiten. Es dient nicht dazu, die im Vorfeld zu ergreifenden Sicherheitsmassnahmen zu beschreiben oder zu konzeptionieren – für diese Fragen wird zum Zeitpunkt des Aufbaus der ICT Netz-Architektur ein Sicherheitskonzept erarbeitet.

## Geltungsbereich und Anwendungsbereich

Dieses ICT Krisenkonzept ist gültig mit der Inkraftsetzung und kommt im Falle einer Krise (eines Incidents) zur Anwendung. Es dient als Grundlage für das Interventions-Teams an der Schule zur Eingrenzung des Incidents, zur Identifikation der betroffenen Netzwerk-Teile, zur Adressierung der involvierten Ansprechstellen und schliesslich zur Festlegung der notwendigen Sofortmassnahmen.

## Definition wichtiger Begriffe

Fügen Sie hier die an Ihrer Schule relevanten ICT-Komponenten und eventuellen Organisations-Einheiten ein, die im Falle eines Incidents wichtig sein könnten:

|  |  |  |
| --- | --- | --- |
| Begriff | Erklärung | Bemerkungen |
| ICT-SPOC | (=Single Point of Contact) Ansprechpartner seitens Gemeinde für ICT-Belange | Hans Muster+41 58 123 12 12 |
| Serverraum "Altbau" | Serverraum im Schulhaus "Meieli", 1. UG, Zimmer 123 | Zugang über Passepartout |
|  |  |  |

1. Bestandesaufnahme

# Infrastruktur

## Netzwerk-Infrastruktur

Ergänzen Sie hier einen Beschrieb der Netz-Infrastruktur, wie sie im Sicherheitskonzept oder im ICT-Architektur-Konzept beschrieben ist. Hilfreich ist hier zudem ein Netzwerkplan.

## Netzwerk-Komponenten

Ergänzen Sie hier die zentralen Netzwerk-Komponenten, die im Falle eines Incidents betroffen sein könnten. Hier sind insbesondere Elemente wie: Router, Netzwerk-Übergänge, Netzwerk-Funktionalitäten und Server relevant.

## Endgeräte

Beschreiben Sie hier die Art der Endgeräte und wie sie in der Netzwerk-Architektur angebunden sind, resp. eingebunden werden können. Beschreiben Sie insbesondere, ob und wie BYOD (=Bring Your Own Device) in das Netz eingebunden werden kann.

# Vertragsmanagement

Führen Sie hier alle Verträge inkl. Lieferanten auf, die Teile oder Komponenten Ihres Schul-Netzwerks mittels Dienstleistung verwalten oder verantworten. Ergänzen Sie auch Support-Kontakte der Lieferanten.

# Schutz der Netz-Infrastruktur

## Netzwerkzugangskontrolle

Beschreiben Sie hier, mit welchen Instrumenten der Zugang zum Netz – virtuell und physisch – ermöglicht wird. Dies erlaubt Ihnen, rasch mögliche Eintritts-Pforten zu identifizieren.

## Segmentierung und Verwaltung von Subnetzen

Kennt die ICT-Architektur eine Segmentierung in Subnetze, deren Übergänge besondere Sicherheitsmassnahmen umfassen, können Sie diese hier beschreiben.

## Schutz gegen externe Angriffe (Firewalls, IPS/IDS etc.)

Führen Sie hier aus, welche netzinternen oder netzexternen Sicherheits-Komponenten im Einsatz sind. Vermerken Sie auch allfällige Zugangs- oder Kontakt-Informationen an dieser Stelle.

# Schutz der Netzwerk-Komponenten

## Sicherheitsrichtlinien für Server

Beschreiben Sie hier, welche Sicherheitsrichtlinien für spezifische Server-Infrastrukturen bestehen.

## Verwaltung von Netzwerkgeräten

Beschreiben Sie hier, wie bestimmte Netzwerk-Geräte wie Router oder WLAN-Hotspots verwaltet werden. Geben Sie zudem an, durch wen die entsprechenden Komponenten verwaltet werden.

## Patch-Management

Falls Sie ein automatisches, halbautomatisches oder manuelles Patch-Management nutzen, können Sie hier den Prozess und die Verantwortlichkeiten beschreiben.

## Physische Sicherheit

Formulieren Sie hier den Zugang und die Zutrittsberechtigung zu den zentralen Netzwerkkomponenten wie Routern, WLAN-Hotspots, Servern, etc.

# Schutz der Endgeräte\*\*

## Richtlinien für Endgeräte

Beschreiben Sie, welche Richtlinien für den Zugang von Endgeräten an Ihrer Schule gelten.

## Verschlüsselung und Sicherheitssoftware

Sollte eine besondere Verschlüsselung für den Traffic innerhalb der Schule zu spezifischen Diensten ausserhalb der Schule bestehen, können Sie diese hier ergänzen.

Ist eine spezifische Sicherheits-Software (Firewall, Content-Filter) auf Schulgeräten installiert, beschreiben Sie hier Ausführung, Funktionsgrad und Implementierung.

## Mobile Gerätemanagement (MDM)

Beschreiben Sie das Produkt, die Ausbreitung und allfällige Sicherheits-Spezifika eines Mobile-Device-Management-Systems, das an Ihrer Schule zum Einsatz kommt.

## BYOD-Richtlinien

Geben Sie an, ob BYOD genutzt wird und wenn ja: wie nicht schuleigene Endgeräte (Laptops, Smartphones, etc.) Zugriff auf das schuleigene Netzwerk erhalten.

## Sicherheitsanforderungen für schuleigene Geräte

Sollte es spezifische Vorgaben zu Sicherheitsanforderungen für den Einsatz von schuleigenen Endgeräten geben (z. B. Finger-Abdruck-Leser, built-in Camera, etc.) führen Sie diese hier aus.

## Trennung privater und schulischer Daten

Falls Sie ein Modell verwenden, das es SuS sowie Lp erlaubt, private und schulische Nutzungs-Profile auf ihrem Gerät einzurichten, beschreiben Sie die Verwendung dieser Option.

# Datenmanagement und Backups

##  Backup-Konzept

Beschreiben Sie, welche Daten in welcher Art gesichert werden. Dabei ist insbesondere die Frequenz, die Lokalität und der Zugriff auf diese Backups relevant.

##  Speicherung und Archivierung von Daten

Sollte es weitere (physikalische, nicht netzbasierte, nicht automatisierte) Sicherungen von Daten geben: Beschreiben Sie hier den entsprechenden Prozess und Ablauf inkl. Ansprechpersonen und Verfügbarkeit.

##  Wiederherstellung im Notfall

Klären Sie mit den verantwortlichen Stellen, wie im Fall eines Incidents auf einen Backup-Satz zugegriffen werden kann, wie ein Recovery ablaufen wird und wie die Integrität der wiederhergestellten Daten validiert werden kann.

1. Organisation und Krise

# Risikoanalyse und -bewertung

## Formen der Sicherheitsrisiken

Formulieren Sie hier die möglichen Sicherheitsrisiken. Eine Auswahl an Risiken finden Sie nachfolgend:

|  |  |  |
| --- | --- | --- |
| Risiko | Beschrieb | Würdigung (relevant/nicht relevant; hoch-mittel-gering) |
| Datenschutz-verletzungen  | Unberechtigter Zugriff auf persönliche Daten von Schüler\*innen, Lehrpersonen und Verwaltungspersonal. |  |
| Cyberangriffe  | Darunter fallen Phishing, Malware, Ransomware-Angriffe und andere Formen von Cyberattacken, die darauf abzielen, das Schulnetzwerk zu infiltrieren. |  |
| Datenverlust  | Verlust wichtiger Daten durch technische Defekte, menschliches Versagen oder durch Cyberangriffe. |  |
| Unzureichende Datensicherung  | Fehlende oder ungenügende Back-up-Verfahren, die im Fall eines Datenverlusts keine Wiederherstellung ermöglichen. |  |
| Missbrauch von ICT-Ressourcen  | Nutzung der Schul-ICT für unangebrachte oder illegale Aktivitäten durch Schüler\*innen oder Personal. |  |
| Software-Risiken  | Verwendung veralteter oder nicht lizenzierter Software kann zu Sicherheitslücken und rechtlichen Problemen führen. |  |
| Hardware-Ausfall  | Versagen von kritischen Systemen oder Geräten, das zu Unterbrechungen im Unterricht oder in der Verwaltung führen kann. |  |
| Unzureichende Netzwerk-sicherheit  | Mangelhafter Schutz des Netzwerks vor unbefugtem Zugriff oder Missbrauch. |  |
| Mangel an Benutzer-schulung  | Lehrpersonen, Schüler\*innen und Verwaltungspersonal sind nicht ausreichend im sicheren und verantwortungsvollen Umgang mit ICT geschult. |  |
| Physische Sicherheits-risiken  | Unzureichende Sicherung von ICT-Geräten vor Diebstahl, Vandalismus oder Naturkatastrophen. |  |
| Unange-messener Online-Inhalt  | Zugang zu potenziell schädlichen oder unangemessenen Materialien im Internet. |  |
| Compliance-Risiken  | Verletzungen gesetzlicher oder behördlicher Anforderungen bezüglich Datenschutz und Datensicherheit. |  |
| Abhängigkeit von Dritt-dienstleistern  | Störungen von Diensten, die von aussen bezogen werden (wie Internetanbieter, Cloud-Services). |  |
| Interoperabili-tätsprobleme  | Schwierigkeiten bei der Integration neuer Technologien in eine bestehende ICT-Struktur oder mangelnde Kompatibilität unter verschiedenen Systemen und Anwendungen. |  |
| Social Engineering  | Taktiken, bei denen Mitarbeitende oder Schüler\*innen dazu verleitet werden, vertrauliche Informationen preiszugeben. |  |
| Insider-Bedrohungen  | Risiken, die von Personen innerhalb der Organisation ausgehen, sei es durch Vorsatz oder Unachtsamkeit. |  |

## Schwachstellen-Analyse

Nehmen Sie eine Analyse vor, welche die oben aufgeführten relevanten/hohen Risiken genauer beschreibt. Dabei sollten Sie Dimensionen wie Gravität, Eintretenswahrscheinlichkeit, Anzahl der betroffenen Personen oder finanzielle Risiken adressieren.

# Sensibilisierung und Schulung

## Festlegung der Verantwortlichkeiten

Definieren Sie für die Schule die verantwortliche Stelle für die Sensibilisierung aller Zielgruppen an Ihrer Schule. Diese Rolle zeichnet verantwortlich, dass die Gruppen in regelmässigen Abständen über mögliche Risiken informiert werden. Definieren Sie die Art und Weise und die Frequenz dieser Sensibilisierungs-Massnahmen und sehen Sie fallweise ein entsprechendes Budget vor.

# Sicherheitsaudits und -bewertungen

Legen Sie fest, in welcher Frequenz, in welchem Modus und durch wen ein Sicherheitsaudit für Ihre Schule durchgeführt werden soll. Als Schule haben Sie die Möglichkeit, ein solches Audit selbst durchzuführen, Ihre ICT-Provider damit zu beauftragen oder eine spezialisierte dritte Partei damit zu beauftragen.

# Massnahmen während und nach einem Incident

## Interventions-Team

Etablieren Sie – analog des Krisen-Interventions-Teams – eine überschaubare Gruppe an Personen und Funktionen, die im Falle eines Incidents die ersten Schritte (siehe unten, [12.2 Sofortmassnahmen definieren](#_Sofortmassnahmen_definieren)) koordinieren. Beschreiben Sie an dieser Stelle auch die Übungsfrequenz und den Übungsmodus dieser Gruppe.

Bereits vor der Aktivierung des Interventions-Teams sollten die wichtigsten Verantwortlichkeiten geklärt werden. Dies betrifft insbesondere die Rolle der Leiterin/des Leiters des Interventions-Teams, die Rolle der Kommunikation oder der Einbezug der Gemeinde. Klären Sie auch Stellvertretungen.

## Interne Hilfestellungen

Identifizieren Sie (im Rahmen einer Übung) weitere interne Know-How-Träger\*innen, die Sie im Falle eines Incidents zum Interventions-Team hinzuziehen können.

## Externe Hilfestellungen

Es bestehen diverse Dienstleister, die ein sogenannten CSIRT-as-a-Service anbieten. Dabei werden im Vorfeld Informationen wie in diesem Dokument aufgeführt und weitere mit dem Anbieter ausgetauscht. In diesem Zusammenhang wird oft auch ein Audit durchgeführt, das Ihnen hilft, Risiko-Felder zu identifizieren und zu beheben.
Beschreiben Sie hier, in welchen Fällen und in welcher Art auf die CSIRT-Ressourcen zugegriffen werden soll und kann. Klären Sie auch ab, wer im Falle eines Beizugs als SPOC fungiert.

Es bestehen diverse Dienstleister, die ein Rapid-Response-Angebot formulieren. Solche Anbieter stellen Ihnen im Falle eines Incidents ein Expert\*innen-Team zur Verfügung, das Sie bei der Bewältigung der Krise namhaft unterstützt. Klären Sie ab, welche Aufgaben und Verantwortungen im Falle eines Beizugs eines Rapid-Response-Teams wo angesiedelt werden.

## Informations-Bedarf

Schenken Sie der Aufgabe, die betroffenen und zu involvierenden Stellen in der nötigen Dringlichkeit und Präzision zu informieren, grosse Aufmerksamkeit. Beschreiben Sie hier die möglichen Interessen-Gruppen und deren Informationsbedarf.

## Informations-Ressourcen

Identifizieren Sie alle relevanten Informationen, die Sie im Falle eines Incidents benötigen, oder die Ihnen bei der Bewältigung der Aufgaben helfen könnten. Strukturieren Sie die Informationsquellen hierarchisch (Gemeinde, Kanton, Bund) und thematisch (Prozesse, Technik, Kommunikation, etc.)

# Situationsanalyse und Sofortmassnahmen

## Identifikation betroffener Daten

Sobald Sie Hinweise oder Verdachte haben, dass ein Incident eingetreten ist, versuchen Sie so rasch als möglich einzugrenzen, welche Daten vom Incident betroffen sind. Die in Kapitel 1 unter 4.2 Segmentierung und Verwaltung von Subnetzen festgehaltenen Informationen helfen dabei, einzelne betroffene Subnetze zu isolieren.

## Sofortmassnahmen definieren

1. **Nicht betroffene Daten sichern.** Sind nur Teile der Daten betroffen, sichern Sie den Zugang zu den übrigen Daten hinsichtlich der eingetretenen Gefahr zusätzlich. Nehmen Sie beispielsweise andere Server vom Netz, sperren Sie Logins von betroffenen Endgeräten oder ändern Sie Passwörter, etc.
2. **Erstellen Sie einen Rapport** über den Incident zusammen mit dem Interventions-Team. Diesen Rapport sollten Sie während der Krise regelmässig aktualisieren und bei Bedarf über die sinnvollen Informationskanäle verbreiten. So stellen Sie sicher, dass alle involvierten Stellen jederzeit über die neuesten Informationen verfügen.
3. **Informations-Konzept erstellen.** Legen Sie fest, wer welche Informationen zu welchem Zeitpunkt benötigt. Unterschätzen Sie diese Aufgabe nicht und stellen Sie genügend personelle Ressourcen für diese Aufgabe zur Verfügung. Achten Sie zudem darauf, dass Sie auf einen Informationskanal zurückgreifen, der nicht vom Incident betroffen ist, und dennoch Vertrauen bei den Empfänger\*innen geniesst (z. B. keine private, sondern eine offizielle E-Mail-Adresse für den Versand verwenden).
4. **Zuhilfenahme interner und externer Hilfe.** Ja nach Organisation Ihrer ICT-Netzwerke sind bestimmte Informationen an unterschiedlicher Stelle verortet. Informieren Sie die Stellen umgehend mit einem Rapport. Die unter 4 Schutz der Netz-Infrastruktur aufgeführten Ressourcen helfen Ihnen dabei, im Krisenfall die richtigen Entscheide zu treffen.
5. **Richtlinien und Verhaltens-Anweisungen.** Erstellen Sie für das Interventions-Team, die Schulbehörde, den Lehrkörper, die SuS und allenfalls die Eltern/Erziehungsberechtigten Verhaltensregeln fest (bei Bedarf). Diese sollen dazu dienen, den Schaden einzugrenzen und ggf. Beweismittel und Indikationen zu identifizieren.
6. Dokumentation und Reporting

## Dokumentation zum ICT-Sicherheitskonzept

Beschreiben Sie hier die verschiedenen Dokumentations-Prozesse, insbesondere:

1. Erstellung und Aktualisierung des Dokuments
2. Frequenz der Überprüfung der hier aufgeführten Informationen (Kontakt-Informationen, Verträge, Produkt-Beschriebe, etc.)
3. Dokumentation im Falle eines Incidents

## Reporting-Mechanismen

Beschreiben Sie hier, wie und in welcher Form Daten über Traffic, aufgerufene Websites, Anmelde-Protokolle, usw. erhoben, analysiert, gespeichert, archiviert und verwendet werden sollen.

1. Anhänge

# Kontaktlisten

# Produkt-Dokumentationen

# Reportings

# Mitglieder des Kriseninterventions-Teams