

Verfahrensdokumentation  
IServ

*Hier bitte den Namen der Schule eintragen*

Stammordner

**Historie**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Datum** | **Geänderte Kapitel/Gliederung** | **Bemerkungen** | **Abnahme Datum/Namenskürzel** |
|  |  |  |  |  |
| 1.0 | 01.4.2019 | Neufassung | Basiert auf der Version von 2013 | 12.4.2019/hjv |
| 2.0 | 1.8.2019 |  | Anpassung an DSGVO und geänderte Programme | 1.8.2019 hjv |
| 2.1 | 7.11.2019 |  | Änderung Gliederung | 7.11.2019 |
| 2.2 | 27.5.2020 |  | Anpassungen für bundesweiten Gebrauch | 28.5.2020 hjv |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Die Grundlage für eine modulare, übersichtliche und leicht zu erweiternde Dokumentations-struktur bildet dieser übergeordnete Ordner, der die allgemeinen Konzepte, Verzeichnisse und Anweisungen enthält. Dieser „Stammordner“ verweist in seinen einzelnen Gliederungspunk-ten auf eventuell vorhandene speziellere Dokumentationen.

Die Struktur ist angelehnt an die Empfehlungen des Datenschutzzentrums Schleswig-Holstein.

[A Sicherheitskonzept 4](#_Toc24019023)

[I Einleitung / Präambel 4](#_Toc24019024)

[II Sicherheitsziele 4](#_Toc24019025)

[III Risiken 6](#_Toc24019026)

[1. Höhere Gewalt 6](#_Toc24019027)

[2. Organisatorische Mängel 6](#_Toc24019028)

[3. Technische Mängel 9](#_Toc24019029)

[4. Menschliche Fehlhandlungen 11](#_Toc24019030)

[5. Vorsätzliche Handlungen 13](#_Toc24019031)

[IV Sicherheitsmaßnahmen 14](#_Toc24019032)

[1. Allgemeines Sicherheitskonzept 14](#_Toc24019033)

[a. Höhere Risiken höherer Gewalt werden folgendermaßen abgesichert: 14](#_Toc24019034)

[i. Brandschutz 14](#_Toc24019035)

[ii. Wasserschutz 15](#_Toc24019036)

[b. Räume und Gebäude 15](#_Toc24019037)

[2. IT-Sicherheitskonzept 17](#_Toc24019038)

[a. Einleitung 17](#_Toc24019039)

[b. IT-Koordination und Berechtigungen 17](#_Toc24019040)

[c. Rechtliche Grundlagen der Datenverarbeitung 18](#_Toc24019041)

[d. Netzwerk / Netzwerkübersicht 19](#_Toc24019042)

[i. Server 21](#_Toc24019043)

[ii. 22](#_Toc24019044)

[iii. Arbeitsplatz-PCs 22](#_Toc24019045)

[iv. Standardsoftware und sonstige Software 23](#_Toc24019046)

[v. Mobile Geräte und Datenträger 23](#_Toc24019047)

[e. Administration 24](#_Toc24019048)

[f. Notfallvorsorge 25](#_Toc24019049)

[i. Notfallplan 25](#_Toc24019050)

[ii. Datensicherung 25](#_Toc24019051)

[iii. Benutzer 26](#_Toc24019052)

[V Restrisikoanalyse und Abhilfemaßnahmen 26](#_Toc24019053)

[B Allgemeines 27](#_Toc24019054)

[I Datenschutzerklärung Internet / Datenschutz-policy 27](#_Toc24019055)

[II Übersicht Fachverfahren 28](#_Toc24019056)

[III Verträge (Kauf, Wartung Auftragsverarbeitung) 29](#_Toc24019057)

[IV Aus- und Fortbildung 29](#_Toc24019058)

[V Dienstanweisungen (allgemein und bezüglich Internet) 29](#_Toc24019059)

[VI Datenschutz- und Sicherheitsmanagement 30](#_Toc24019060)

[1. Datenschutzbeauftragter 30](#_Toc24019061)

[2. Regelmäßige Kontrollen 30](#_Toc24019062)

[3. Anlassbezogene Kontrollen 30](#_Toc24019063)

[4. Verhalten bei Sicherheitsvorfällen 30](#_Toc24019064)

[5. Integration von Datenschutz und Datensicherheit 31](#_Toc24019065)

# 

# Sicherheitskonzept

## Einleitung / Präambel

Das Internet mit seinen Möglichkeiten zum weltweiten schnellen Beschaffen und Aus­tauschen von Informationen jeglicher Art ist für viele Schulbereiche unverzichtbar geworden.

Aber auch der lokale Einsatz der Informationstechnologie zur effizienteren Gestaltung des Unterrichts oder zur Beschleunigung von Arbeitsabläufen ist aus der Schule nicht mehr wegzudenken.

Es wächst aber auch die Abhängigkeit vom reibungslosen Funktionieren der Technik. Ein auch nur kurzfristiger Ausfall des Schulnetzes bedeutet bereits für viele eine spürbare Behinderung. Umso wichtiger ist es, Sicherheit und Zuverlässigkeit zu planen und zu prüfen.

Es muss entschieden werden, welche Risiken man einzugehen bereit ist und gegen welche Risiken man Maßnahmen ergreifen möchte. Zu diesem Zweck muss zunächst definiert werden, was die schützenswerten Güter sind und analysiert werden, welche Gefahren ihnen drohen.

Das vorliegende Sicherheitskonzept definiert das Verhältnis dieser Schule zu Sicherheits­fragen der von ihr eingesetzten Informationstechnik. Es benennt die Gefährdungen und schlägt ggf. geeignete Präventionsmaßnahmen vor. Es besteht aus zwei Teilen:

Teil A: Sicherheitskonzept (Sicherheitsziele, Risiken, Sicherheitsmaßnahmen)

Teil B: Allgemeines

Dieses Sicherheitskonzept beschreibt im Detail die technischen und organisatorischen Maßnahmen unserer Schule, die bei jeder Verarbeitung personenbezogener Daten gelten und regelt die Verantwortlichkeiten und Aufbau- bzw. Ablauforganisation dieser Schule in der Informations- und Kommunikationstechnologie.

Es beschreibt weiterhin Prozesse und Vorgehensweisen zur Errichtung und Inbetriebnahme von neuen Fachverfahren.

Dieses Konzept ist angelehnt an den IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik.   
  
Zu finden unter: <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html>

## Sicherheitsziele

Diese Schule betreibt die automatisierte Datenverarbeitung mit den folgenden festgelegten Sicherheitszielen:

* Beachten und Umsetzen der Rechtmäßigkeit und Ordnungsmäßigkeit der Datenverarbeitung
* Wahrung und Schutz des Grundrechts der Betroffenen auf informationelle Selbstbestimmung
* Datenminimierung bei der Datenverarbeitung
* Sicherstellen der Verfügbarkeit der durch diese Schule verwendeten Systeme und Programme
* Aufrechterhalten der Integrität der Systeme und insbesondere der gespeicherten personenbezogenen Daten
* Gewährleisten der Vertraulichkeit der in dieser Schule verarbeiteten Daten
* Beachten von wirtschaftlichen Obliegenheiten

*Die Sicherheitsziele können/sollten schulindividuell geprüft und ggf. erweitert werden.*

## Risiken

Die Aufrechterhaltung der oben erwähnten Sicherheitsziele kann durch die folgenden Sachverhalte gefährdet sein:

### Höhere Gewalt

***Fragestellung: Kann die Informations- und Kommunikationstechnologie dieser Schule durch höhere Gewalt in ihrer Funktion beeinträchtigt werden oder komplett ausfallen?***

Folgende Risiken höherer Gewalt könnten eintreten:

* Blitzeinschlag
* Überspannung
* Feuerschäden
* Wasserschäden
* Sturmschäden
* Schneemassenschäden
* Personalausfall
* Kabelbrand
* Unzulässige Temperatur und Luftfeuchte
* Staub, Verschmutzung
* Datenverlust durch starke Magnetfelder
* Technische Katastrophen im Umfeld
* Beeinträchtigung durch wechselnde Einsatzumgebung
* Ausfall oder Störung eines Funknetzes
* Ausfall eines Gebäudes
* Ausfall eines Dienstleisters oder Zulieferers

### Organisatorische Mängel

***Fragestellung: Kann die Informations- und Kommunikationstechnologie dieser Schule durch organisatorische Mängel in ihrer Funktion beeinträchtigt werden oder komplett ausfallen?***

Folgende mögliche organisatorische Mängel könnten eintreten:

* Fehlverhalten bei Schülerinnen, Schülern und Mitarbeiterinnen und Mitarbeitern dieser Schule durch fehlende oder nicht ausreichende Regelungen oder durch unzureichende Kenntnis der Regelungen
* Beeinträchtigung der Vertraulichkeit oder die Integrität von personenbezogenen Daten, z. B. durch falsche Berechtigungsvergabe
* Verstoß gegen geltende rechtliche Bestimmungen bei der Verarbeitung personen­bezogener Daten durch diese Schule
* Beeinträchtigung der Vertraulichkeit und Integrität der personenbezogenen Daten sowie der Verfügbarkeit der verwendeten Programme und Systeme, z. B. durch den unkontrollierten Zugriff durch externe Personen auf die Information- und Kommu­nikations­technologie dieser Schule
* Beeinträchtigung der Sicherheitsziele dieser Schule durch fehlerhafte oder nicht aus­reichende Planung und Konzeption beim Einsatz der zur Verfügung stehenden Sicher­heitsmechanismen der eingesetzten IT-Technologie
* Unberechtigte Einsichtnahme oder Veränderung personenbezogener Daten durch unzu­reichende Regelungen und Verträge im Rahmen einer Auftragsverarbeitung
* Unbefugter Zutritt zu schutzbedürftigen Räumen
* Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
* Nicht fristgerecht verfügbare Datenträger
* Unzureichende Dokumentation der Verkabelung
* Unzureichend geschützte Verteiler
* Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
* Ungeordneter Benutzerwechsel
* Mangelhafte Kennzeichnung der Datenträger
* Ungeregelte Weitergabe von Datenträgern
* Unzureichendes Schlüsselmanagement bei Verschlüsselung
* Fehlende Auswertung von Protokolldaten
* Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
* Fehlende oder unzureichende Dokumentation
* Verstöße gegen das Urheberrecht
* Unzureichende Leitungskapazitäten
* Ungeeignete Einschränkung der Benutzerumgebung
* Unkontrollierter Aufbau von Kommunikationsverbindungen
* Fehlende oder unzureichende Aktivierung von Datenbank Sicherheitsmechanismen
* Mangelhafte Konzeption des Datenbankzugriffs
* Mangelhafte Organisation des Wechsels von Datenbank-Benutzern
* Inkompatible aktive und passive Netzkomponenten
* Konzeptionelle Schwächen des Netzes
* Überschreiten der zulässigen Kabel- bzw. Bus-Länge oder der Ringgröße
* Ungesicherter Akten- und Datenträgertransport
* Ungeeignete Entsorgung der Datenträger und Dokumente
* Erhöhte Reaktionszeiten bei IT-Systemausfall
* Vertraulichkeitsverlust durch Restinformationen
* Mangelhafte Beschreibung von Dateien
* Nicht ausreichende Speichermedien für den Notfall
* Betreiben von nicht angemeldeten Komponenten
* Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement
* Unberechtigte Sammlung personenbezogener Daten
* Ungeeigneter Umgang mit Sicherheitsvorfällen
* Fehlende Regelungen für das RAS-System
* Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
* Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen
* Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches
* Unzureichende Notfallvorsorge bei einem Sicherheitsgateway
* Unzureichende Sensibilisierung für Informationssicherheit
* Unzureichende Schulung der Schülerinnen, Schüler und Mitarbeiterinnen und Mitarbeiter
* Inkompatibilität zwischen fremder und eigener IT
* Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen
* Störung der Arbeitsabläufe aufgrund von Sicherheitsvorfällen
* Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheits­management
* Fehlende oder unzureichende Planung des Speichersystems
* Fehlende oder unzureichende Planung des WLAN-Einsatzes
* Unzureichende Regelungen zum WLAN-Einsatz
* Ungeeignete Auswahl von WLAN-Authentifikationsverfahren
* Ungeeignete Aufstellung von sicherheitsrelevanten IT-Systemen
* Unzureichende Kontrolle von WLANs
* Fehlende Übersicht über den Informationsverbund
* Mangelhafte Berücksichtigung von mobilen Endgeräten beim Patch- und Änderungs­management
* Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungsmanagement
* Nicht erkannte Sicherheitsvorfälle
* Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen

### Technische Mängel

***Fragestellung: Kann die Informations- und Kommunikationstechnologie dieser Schule durch technische Mängel in ihrer Funktion beeinträchtigt werden oder komplett ausfallen?***

Folgende mögliche technische Mängel könnten eintreten:

* Beeinträchtigung der Integrität und Verfügbarkeit sowohl der verwendeten IT-Technologie als auch der personenbezogenen Daten durch Fehlfunktionen der eingesetzten Programme und Systeme
* Ungenügende Anforderung der eingesetzten Programme und Systeme in Bezug auf die Sicherheitsziele
* Ausfall der Stromversorgung
* Ausfall interner Versorgungsnetze
* Ausfall vorhandener Sicherungseinrichtungen
* Spannungsschwankungen/Überspannung/Unterspannung
* Defekte Datenträger
* Ausfall der internen Stromversorgung
* Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
* Verlust gespeicherter Daten
* Überlastung von Informationssystemen
* Software-Schwachstellen oder -Fehler
* Ausfall einer Datenbank
* Unterlaufen von Zugriffskontrollen über ODBC
* Verlust von Daten einer Datenbank
* Datenverlust einer Datenbank bei erschöpftem Speichermedium
* Verlust der Datenbankintegrität/-konsistenz
* Ausfall oder Störung von Netzkomponenten
* Nichtzustellung einer Nachricht
* Schlechte oder fehlende Authentifikation
* Mangelnde Verlässlichkeit von Groupware
* Ausfall von Komponenten eines Netz- und Systemmanagementsystems
* Software-Konzeptionsfehler
* Nicht dokumentierte Funktionen
* Ausfall der Systeme eines Outsourcing-Dienstleisters
* Unsichere Default-Einstellungen auf Routern und Switches
* Unsichere Default-Einstellungen bei Speicherkomponenten
* Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen
* Verwendung unzureichender Steckdosenleisten
* Verstaubte Lüfter
* Komplexität von Druckern, Kopierern und Multifunktionsgeräten
* Unzureichender Schutz der Kommunikation bei Druckern und Multifunktionsgeräten
* Beeinträchtigung von Gesundheit und Umwelt durch Drucker, Kopierer und Multifunktionsgeräte
* Ausfall von Verzeichnisdiensten

### Menschliche Fehlhandlungen

Zahlreiche Untersuchungen und Statistiken über Fehlfunktionen im IT-Bereich zeigen, dass die größten Risiken durch Irrtum, menschliches Versagen und Überforderung der Nutzer entstehen. Daher sind die in diesem Abschnitt aufgeführten Maßnahmen vorrangig zu beachten.

Folgende mögliche menschliche Fehlhandlungen könnten eintreten:

* Nichtbeachten der getroffenen Weisungen durch die Schülerinnen, Schüler und Mitarbeiterinnen und Mitarbeiter dieser Schule
* Beeinträchtigung der Sicherheitsziele durch fahrlässiges Verhalten der Schülerinnen, Schüler und Mitarbeiterinnen und Mitarbeiter dieser Schule
* Nicht sachgerechte oder angemessene Nutzung der zur Verfügung gestellten Funktionen der Informations- und Kommunikationstechnologie durch Schülerinnen, Schüler und Mitarbeiterinnen und Mitarbeiter dieser Schule
* Beeinträchtigung der Integrität und Verfügbarkeit sowohl der verwendeten Informations- und Kommunikationstechnologie als auch der personenbezogenen Daten durch fehler­hafte oder unzureichende Ausübung von festgelegten administrativen Rechten
* Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
* Gefährdung durch Reinigungs- oder Fremdpersonal
* Verlust der Datenträger beim Versand
* Weitergabe falscher oder interner Informationen
* Fehlerhafte Administration von Zugangs- und Zugriffsrechten
* Kein ordnungsgemäßer PC-Benutzerwechsel
* Fehlerhafte Änderung der Registrierung
* Fahrlässiges Löschen von Objekten
* Ungewollte Freigabe des Dateisystems
* Ungeeignete Konfiguration der aktiven Netzkomponenten
* Fehlende oder ungeeignete Segmentierung
* Server im laufenden Betrieb ausschalten
* Fehlinterpretation von Ereignissen
* Konfigurations- und Bedienungsfehler
* Ungeeigneter Umgang mit Passwörtern
* Sorglosigkeit im Umgang mit Informationen
* Unzureichende Identifikationsprüfung von Kommunikationspartnern
* Fehler bei der Synchronisation mobiler Endgeräte
* Mangelhafte Akzeptanz von Informationssicherheit
* Fliegende Verkabelung
* Fehler bei der Synchronisation von Datenbanken
* Fehlerhafte Konfiguration der WLAN-Infrastruktur
* Ungeregelte und sorglose Nutzung von Druckern, Kopierern und Multifunktionsgeräten
* Fehlerhafte Konfiguration von Verzeichnisdiensten
* Falsche Vergabe von Zugriffsrechten
* Falscher Umgang mit defekten Datenträgern
* Ungenehmigte Nutzung von externen Dienstleistungen
* Ungeeignetes Verhalten bei der Internet-Nutzung
* Rufschädigung

### Vorsätzliche Handlungen

***Fragestellung: Kann die Informations- und Kommunikationstechnologie dieser Schule durch vorsätzliche Handlungen in ihrer Funktion beeinträchtigt werden oder komplett ausfallen?***

Folgende mögliche vorsätzliche Handlungen könnten eintreten:

* Diebstahl
* Vorsätzliches Fehlverhalten der Schülerinnen, Schüler und Mitarbeiterinnen und Mitarbeiter dieser Schule, insbesondere der Administratoren
* Angriffe und Manipulationen durch betriebsexterne Personen
* Manipulation oder Zerstörung von Geräten oder Zubehör
* Manipulation an Informationen oder Software
* Unbefugtes Eindringen in ein Gebäude
* Vandalismus
* Anschlag
* Abhören von Leitungen
* Manipulation an Leitungen
* Unberechtigte IT-Nutzung
* Missbrauch von Fernwartungszugängen
* Gefährdung bei Wartungs-/Administrierungsarbeiten
* Systematisches Ausprobieren von Passwörtern
* Missbrauch von Benutzerrechten
* Missbrauch von Administratorrechten
* Trojanische Pferde
* Diebstahl bei mobiler Nutzung des IT-Systems
* Schadprogramme
* Unberechtigtes Kopieren der Datenträger
* Eindringen in Rechnersysteme über Kommunikationskarten
* Abhören von Räumen mittels Rechner mit Mikrofon und Kamera
* Makro-Viren
* Missbrauch von Administratorrechten bei Windows-Betriebssystemen
* Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit
* Vorsätzliches Herbeiführen eines Abnormal End
* Umgehen der Systemrichtlinien
* Missbrauch von Remote-Zugängen für Managementfunktionen von Routern
* Unberechtigter Anschluss von IT-Systemen an ein Netz
* Unberechtigte Ausführung von Netzmanagement-Funktionen
* Unberechtigter Zugang zu den aktiven Netzkomponenten
* Manipulation durch Familienangehörige und Besucher
* Vertraulichkeitsverlust schützenswerter Informationen
* Missbräuchliche Groupware-Nutzung
* Vortäuschen eines falschen Absenders
* Manipulation von Alias-Dateien oder Verteilerlisten
* Überlastung durch eingehende E-Mails
* Mitlesen von E-Mails

## 

## Sicherheitsmaßnahmen

Folgende Sicherheitsmaßnahmen werden bezüglich der bestehenden oben beschriebenen Risiken ergriffen. Hierbei ist zunächst erheblich, dass in einer Schule grundsätzlich zwei voneinander getrennte Infrastrukturen existieren:

* Verwaltungs- bzw. Landesnetz
* Pädagogisches Netz (IServ)

***Fragestellungen:***

***Was? Beschreibung technischer und organisatorischer Maßnahmen***

***Warum? Für die Aufrechterhaltung der Sicherheitsziele***

***Wie? Gliederung nach welchen Bereichen, Maßnahmen***

Zur Absicherung der beschriebenen Risiken werden folgende Sicherheitsmaßnahmen ergriffen:

### Allgemeines Sicherheitskonzept

Allgemeine Sicherheitsmaßnahmen betreffen die Sicherheitsmaßnahmen, die über die reinen IT-Sicherheitsmaßnahmen hinausgehen.

*Die von der Schule getroffenen oder noch zu treffenden allgemeinen Sicher­heits­maßnahmen sind zu beschreiben. Orientierung bieten die „Fragestellungen“. Die „Formulierungsvorschläge“ können übernommen bzw. als Basis für schulindividuelle Ausführungen genutzt werden.*

#### Höhere Risiken höherer Gewalt werden folgendermaßen abgesichert:

##### Brandschutz

Formulierungsvorschläge:

Die Regeln des vorbeugenden Brandschutzes sind zu beachten und einzuhalten. Insbesondere gilt dies für Räume mit wichtiger Informationstechnik, wie beispielsweise Serverräume. Papierlager, leere Verpackungen und andere leicht entflammbare Materialen dürfen in diesen Räumen nicht gelagert werden. In diesen Räumen sowie in anderen Technikräumen besteht Rauchverbot. Die Türen zu diesen Räumen sollen brandhemmend ausgelegt sein. In diesem Zusammenhang sind die Schutzklassen T30, T60, T90, T120 und T180 zu nennen. Außerdem sind Brandmelder und Handfeuerlöscher (Brandklasse B, CO2-Löscher) vorzusehen. Für Hinweise und eingehende Beratung wenden Sie sich an Ihren örtlichen Brandschutzbeauftragten.

##### Wasserschutz

Formulierungsvorschläge:

IT-Systeme, die wichtige oder unverzichtbare Komponenten zur Aufrechterhaltung eines geordneten Betriebes sind, sind nicht in direkter Nähe zu oder unter wasserführenden Leitungen aufzustellen. Auch bei einem Wassereinbruch muss der weitere Betrieb der IT-Systeme gewährleistet sein, dies gilt insbesondere dann, wenn die IT-Systeme in Kellerräumen aufgestellt werden. So ist beispielsweise besonders darauf zu achten, dass nicht die tiefste Stelle im Gebäude zur Aufstellung der Geräte genutzt wird.

#### Räume und Gebäude

*Fragestellungen:*

***Zutrittskontrolle/Schließanlage:***

* Welche Art Schließanlage wird eingesetzt?
* Wie werden Schlüssel an die jeweils Zutrittsberechtigten vergeben?
* Wird die Vergabe von Schlüsseln dokumentiert? Schlüsselbuch? Verantwortlichkeit?
* Gibt es Schließgruppen?
* Einsatz einer Alarmanlage (z. B. im Erdgeschoss)

***Verhaltensregeln der Mitarbeiter***

* Verschluss der Räume beim Verlassen
* Verschluss der Fenster außerhalb der Geschäftszeiten

***Serverraum***

* Standort für Server und Backupserver beschreiben. Räumliche Trennung darstellen.
* Zugangssicherheit? Alarmanlage? Schlüsselmanagement?
* Wer hat Zugang? Administratoren? Hausmeister? Wachdienst? Putzdienst?
* Protokollierung des Zugangs?
* Videokontrolle des Serverraums?

***Netzwerkinfrastruktur***

* LAN
* Übergabepunkt DSL
* Netzwerkschränke (Was sind das für Schränke? Was ist darin untergebracht? Wo im Gebäude sind die Schränke zu finden? Wer hat die Schlüssel?
* WLAN
* Accesspoints (Was sind das für Accesspoints? Wo im Gebäude sind die Accesspoints zu finden? Dokumentation der Zugangsdaten der Accesspoints*.*

Die Sicherheitsmaßnahmen bezüglich der Räume und Gebäude sind in (z. B. Raumplan) geregelt.

**Beispiel Raumplan**



*Dieses Muster ist gegen den schulindividuellen Raumplan auszutauschen.*

### 

### IT-Sicherheitskonzept

#### Einleitung

Beschaffung, Entwicklung und Einsatz von IT-Anwendungen und -Systemen erfolgt nach Maßgabe der für diese Schule geltenden Regelungen. Zusätzlich sind Regelungen des Landes zu beachten, die eine ordnungsgemäße IT-Organisation, Verfahrensplanung und -realisierung beschreiben, soweit diese für diese Schule verbindlich sind.

*Das IT-Sicherheitskonzept ist schulindividuell zu entwickeln und zu dokumentieren. Orientierung bieten die „Fragestellungen“. Die „Formulierungsvorschläge“ können übernommen bzw. als Basis für schulindividuelle Ausführungen genutzt werden.*

#### IT-Koordination und Berechtigungen

***Fragestellungen:***

***Wie wird der Zugriff auf die IT-Technologie geregelt? Werden allgemeine und/oder spezielle Berechtigungskonzepte eingesetzt?***

***Nach welchem Prinzip wird die Vergabe von Zugriffsberechtigungen geregelt? Minimalprinzip?***

***Wie ist der Prozess zur Vergabe von Berechtigungen? Antrag (Mitarbeiter) – Abstimmung (Fachamt) – Freigabe (Verantwortlicher) – Umsetzung (Administrator) – Kontrolle (Verantwortlicher)***

Allgemeine Vorgaben:

Die Verantwortung für die Umsetzung und Einhaltung der für den IT-Einsatz geltenden Regelungen trägt die Schulleitung.

Der gesamte IT-Einsatz ist in IT-Verfahren zu gruppieren. Jedes Verfahren ist zu beschreiben. Im Abschnitt B II dieses Sicherheitskonzepts werden die wichtigsten Aspekte einer Verfahrensdokumentation zusammengefasst und in den dort aufgeführten einzelnen Verfahrensordnern detailliert beschrieben.

Für jedes IT-Verfahren bzw. jeden IT-Arbeitsprozess sind die Verantwortlichkeiten für alle Bereiche eindeutig festzulegen. Normalerweise ist eine Rollentrennung von Verfahrensentwicklung/-pflege und Systemadministration sinnvoll. Jedem Mitarbeiter müssen die ihm übertragenen Verantwortlichkeiten und die ihn betreffenden Regelungen bekannt sein. Abgrenzungen und Schnittflächen der verschiedenen Anwenderrollen müssen klar definiert sein.

Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Funktionen bevollmächtigt wird, IT-Systeme, IT-Anwendungen oder Daten zu nutzen. Der Benutzer darf nur mit den Zugriffsrechten arbeiten, die unmittelbar für die Erledigung seiner Aufgaben vorgesehen sind.

Im Bereich der Schulverwaltung erfolgt die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer auf schriftlichen Antrag. In allen anderen Bereichen sind die dort geltenden Regelungen zu beachten.

Es ist zu prüfen, inwieweit die Zugriffserlaubnis auf bestimmte Arbeitsplatz-PCs begrenzt werden kann. Für Benutzer mit besonderen Rechten, insbesondere für Administratorkennungen, ist eine Zugriffserlaubnis auf die notwendigen Rechner (i.d.R. sind es der betreffende Server und die Arbeitsplatz-PCs) zu begrenzen. Es ist ebenfalls zu prüfen, inwieweit die Zugangserlaubnis auf bestimmte Zeiten begrenzt werden kann.

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass das zuständige IT-Personal über die notwendige Änderung der Berechtigungen eines Anwenders, z. B. in Folge von Änderungen seiner Aufgaben, rechtzeitig informiert wird, um die Berechtigungsänderungen im System abzubilden.

#### Rechtliche Grundlagen der Datenverarbeitung

Die rechtlichen Grundlagen der Datenverarbeitung sind

* In der Europäischen Datenschutzgrund-Verordnung (DSGVO), im
* Im Bundesdatenschutzgesetz (BDSG-neu)
* Im Landesdatenschutzgesetz Schleswig-Holstein (LDSG) und
* In der Schul-Datenschutzverordnung (SchulDSVO) festgelegt.

Systeme

Formulierungsvorschläge:

Allgemeine Vorgaben:

Alle IT-Systeme, die wichtige oder unverzichtbare Beiträge zur Aufrechterhaltung eines geordneten Betriebes leisten, wie zum Beispiel Server und aktive, zentrale Netzwerk­komponenten, sind an eine unterbrechungsfreie Stromversorgung (USV) zur Überbrückung von Spannungsschwankungen anzuschließen. Die Konfiguration der USV und der durch sie geschützten Systeme muss ein rechtzeitiges und kontrolliertes Herunterfahren der Systeme gewährleisten.

Alle wichtigen anderen IT-Systeme dürfen nur an eine ausreichend dimensionierte und gegen Überspannungen abgesicherte Stromversorgung angeschlossen werden. Bei Einsatz von Geräten mit redundant ausgelegter Stromversorgung ist darauf zu achten, dass die einzelnen Netzteile über getrennt abgesicherte Stromkreise versorgt werden. Die für den Betrieb von IT notwendigen Unterlagen und Informationen zur elektrischen Versorgung sind dem IT-Verantwortlichen auf Anfrage von den IT-Dienstleistern bzw. der IT-Abteilung zur Verfügung zu stellen.

Der Anschluss von Systemen an das Datennetz dieser Schule hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen ohne Absprache mit dem IT-Verantwortlichen des Bereichs und ggf. mit dem Datenschutzbeauftragten ist unzulässig.

Alle IT-Systeme und Anwendungen sind so einzurichten, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist eine Anmeldung mit Benutzerkennung und Passwort erforderlich. Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen soll in der Regel personenbezogen erfolgen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem Benutzer ist untersagt, Kennungen und Passwörter zu dokumentieren oder weiterzugeben.

Redundanzen bei der Benutzerverwaltung sind zu vermeiden. Die Zuordnung von mehreren Kennungen zu einer Person innerhalb eines IT-Systems sollte nur in begründeten Ausnahmefällen erlaubt sein, wie beispielsweise für Systemadministratoren. Die Einrichtung und Freigabe einer Benutzerkennung dürfen nur in einem geregelten Verfahren erfolgen. Die Einrichtung und Freigabe sind zu dokumentieren.

Je nach den Möglichkeiten des Betriebssystems sind alle Zugangsversuche, sowohl die erfolgreichen als auch die erfolglosen, automatisch zu protokollieren. Das Ändern wichtiger Systemparameter und auch das Herunterfahren bzw. das Hochfahren des Systems sollten ebenfalls protokolliert werden.

Die Protokolle sollten regelmäßig und zeitnah ausgewertet werden. Es muss dabei sicherge­stellt sein, dass nur die Personen Zugriff auf die Protokolle erlangen können, die dafür von der zuständigen Stelle mit den nötigen Rechten ausgestattet wurden. Das Prinzip der Zweckbindung ist unbedingt zu beachten.

Bei der Protokollierung durch Anwendungssysteme ist der Grundsatz der Datenvermeidung zu beachten, d.h. es sind so wenig personenbezogene Daten wie möglich zu protokollieren. Von Anwendungssystemen erzeugte Protokolldaten sind vor dem Zugriff Unbefugter zu schützen.

#### Netzwerk / Netzwerkübersicht

Allgemeine Vorgaben:

Vernetzungsinfrastruktur (Switches, Router, Hubs, u. ä.) ist grundsätzlich in verschlossenen Räumen oder in nicht öffentlich zugänglichen Bereichen in verschlossenen Schränken einzurichten, die gegen unbefugten Zutritt und Zerstörung ausreichend gesichert sind. Es gelten die gleichen Empfehlungen wie unter ii (s.u.).

Die Verkabelung des LAN ist klar zu strukturieren sowie aktuell und vollständig zu dokumentieren. Die Netzwerkadministratoren müssen einen vollständigen Überblick über die Kabelverlegung und die Anschlussbelegung zentraler Komponenten haben. Nicht benutzte Anschlüsse sollten abgeklemmt oder deaktiviert werden. Erweiterungen und Veränderungen an der Gebäudeverkabelung, auch die Inbetriebnahme von Funknetzen, sind mit dieser Schule abzustimmen.

Bei der Verlegung der Leitungen muss darauf geachtet werden, dass Unbefugte keine Möglichkeit des Zugriffs haben. Offen zugänglich verlegte Leitungen sollten in Zusammenarbeit mit der für die Baumaßnahmen zuständigen Stelle in geeigneter Weise geschützt werden.

Eine angemessene Protokollierung, Audit und Revision sind wesentliche Faktoren der Netzsicherheit. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise einen Rückschluss, ob die Bandbreite des Netzes den derzeitigen Anforderungen genügt, oder die Erkennung von systematischen Angriffen auf das Netz.

Unter einem Audit wird die Verwendung eines Dienstes verstanden, der insbesondere sicherheitskritische Ereignisse betrachtet. Bei einem Audit werden die Ereignisse mit Hilfe geeigneter Werkzeuge betrachtet und ausgewertet.

Protokolle dienen dem Erkennen und Beheben von Fehlern. Mit ihrer Hilfe lässt sich feststellen, wer wann welche Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit).

Je nach Schutzbedarf des Verfahrens müssen adäquate Maßnahmen zur Protokollierung getroffen werden, um die Revisionsfähigkeit zu gewährleisten.

Bei der Revision werden die beim (Offline-) Audit gesammelten Daten von einem oder mehreren unabhängigen Mitarbeitern (4-Augen-Prinzip) überprüft, um Unregelmäßigkeiten beim Betrieb der IT-Systeme aufzudecken und die Arbeit der Administratoren zu kontrollieren.

Das Netzwerk dieser Schule ist folgendermaßen aufgebaut, was durch die Grafik stark vereinfacht dargestellt wird:

**Beispiel Netzwerkplan**



*Dieses Muster ist gegen den schulindividuellen Netzwerkplan auszutauschen.*

##### Server

Allgemeine Vorgaben:

Alle Rechnersysteme mit typischer Serverfunktion, einschließlich der Peripheriegeräte (Konsolen, externe Platten, Laufwerke u. ä.), sind in separaten, besonders gesicherten Räumen aufzustellen.

Jedes Serversystem ist mit einem RAID-System und redundanten Netzteilen ausgestattet.

Die Daten jedes Servers werden auf Sicherungsmedien in mehreren Generationen gesichert. Die verwendeten Sicherungsmedien werden in einem feuersicheren Tresor aufbewahrt. Lediglich die Administration hat Zugriff auf die Datensicherungsmedien. Für jedes System sind ein Sicherungsplan und eine Anleitung zur Wiederherstellung in der jeweiligen Systemakte hinterlegt.

Jeweils eine Generation der Sicherungsmedien wird ein angemietetes Bankschließfach ausgelagert.

Die Ablage von Daten erfolgt ausschließlich auf den Servern.

Der Zugang Unbefugter zu den Serverräumen muss zuverlässig verhindert werden. Je nach der Schutzbedürftigkeit sowie in Abhängigkeit von äußeren Bedingungen (öffentlicher zugänglicher Bereich, Lage zur Straße usw.) sind besondere bauliche Maßnahmen, wie zum Beispiel einbruchssichere Fenster, einbruchssichere Türen, Bewegungsmelder o. ä. zur Verhinderung von gewaltsamem Eindringen vorzusehen.

Serverräume, in denen besonders schützenswerte Daten gespeichert bzw. verarbeitet werden und die nicht über entsprechende bauliche Sicherungsvorkehrungen verfügen, sollen möglichst unauffällig sein, d. h. Hinweisschilder u. ä. sollten nicht angebracht werden, damit die Funktion der Räume nicht sofort erkennbar wird.

Die Türen dürfen nur durch geeignete Schließsysteme zu öffnen sein und sollen selbsttätig schließen; verwendete Schlüssel müssen kopiergeschützt sein. Für die Schlüsselverwaltung sind besondere Regelungen erforderlich, die eine Herausgabe an Unbefugte ausschließen.

Der Zutritt muss auf diejenigen Personen begrenzt werden, deren Arbeitsaufgaben dieses erfordert. Das Betreten der Räume darf nur nach vorheriger Anmeldung bei der für die Räume verantwortlichen Stelle erfolgen. Reinigungspersonal soll die Serverräume nach Mög­lichkeit nur unter Aufsicht betreten.

Der Einbau von Klimatisierungsanlagen wird erforderlich, wenn der Luft- und Wärme­austausch von Server- und Rechnerräumen unzureichend ist bzw. hohe Anforderungen an die Be- und Entfeuchtung eines Raumes gestellt werden. Die Gewährleistung der zulässigen IT-Betriebstemperatur und demzufolge die Sicherstellung des IT-Betriebs steht in engem Zusammenhang mit dem reibungslosen Einsatz von Klimatisierungsgeräten. Daher müssen die Geräte mit einer hohen Verfügbarkeit ausgestattet sein.

##### 

##### Arbeitsplatz-PCs

Allgemeine Vorgaben:

Die Arbeitsplatz-PCs werden zentral konfiguriert und administriert.

Jeder Arbeitsplatz-PC wird sowohl bei der Erstinstallation als auch bei der weiteren Pflege der installierten Programme über Mechanismen zur automatisierten Softwareverteilung (RIS und Installation von Programmen über MSI-Pakete via Gruppenrichtlinien) mit getesteten und freigegebenen Programmversionen versehen.

Auf allen Arbeitsplatz-PCs ist ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Jede Organisationseinheit ist verpflichtet, Virenschutzsysteme anzubieten. Durch den Einsatz von Virenschutzsystemen soll das Eindringen von schädlichem Programmcode erkannt und verhindert werden.

Regelmäßig (möglichst automatisiert) sind die Virenerkennungsmuster zu aktualisieren.

Wird auf einem System schädlicher Programmcode entdeckt, muss dies der zuständigen Stelle gemeldet und das Ergebnis der eingeleiteten Maßnahmen dokumentiert werden.

Empfehlenswert ist, in regelmäßigen Abständen sowie bei konkretem Bedarf oder Verdacht eine Suche nach Schadprogrammen auf allen bedrohten IT-Systemen vorzunehmen und die Ergebnisse zu dokumentieren.

Bei kürzerem Verlassen des Raumes, d.h. bis ca. 10 Minuten, muss der Zugriff auf das IT-System durch einen Kennwortschutz gesperrt werden. Grundsätzlich sind die Systeme nach der Abmeldung auszuschalten, es sei denn, schulische Anforderungen sprechen dagegen. Soweit es technisch möglich ist, sollte ein Arbeitsplatz-PC so konfiguriert sein, dass nach längerer Inaktivität (beispielsweise 20 Minuten) der PC automatisch gesperrt wird und nur nach erneuter Eingabe eines Passwortes zu aktivieren ist.

##### Standardsoftware und sonstige Software

Allgemeine Vorgaben:

Die Beschaffung von Soft- und Hardware ist mit dem zuständigen IT-Verantwortlichen abzustimmen. Dieser ist für die Einhaltung von Standards und Sicherheitsanforderungen verantwortlich.

Auf Rechnersystemen dieser Schule darf zum Zweck des Schutzes von schuleigener Hardware und dem Schulnetz nur Software installiert werden, die von der zuständigen Stelle dafür freigegeben wurde. Bei der Freigabe muss darauf geachtet werden, dass die Software aus zuverlässiger Quelle stammt und dass ihr Einsatz notwendig ist.

Das eigenmächtige Einspielen, insbesondere auch das Herunterladen von Software aus dem Internet oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn eine Genehmigung der zuständigen Stelle vorliegt oder eine Organisationseinheit eine pauschale Freigabe für Teilbereiche festgelegt hat. Rechnersysteme sind gegen das unbefugte Herunterladen hard- und softwaretechnisch zu schützen.

Vor dem Einsatz neuer Software oder neuer Versionen muss die Erfüllung der Spezifikation durch hinreichende Tests sichergestellt sein. Der Testverlauf und das Testergebnis sind zu dokumentieren.

##### Mobile Geräte und Datenträger

Mobile Geräte

Für mobile Geräte gelten die für die Arbeitsplatz-PCs aufgeführten Sicherheitsmaßnahmen entsprechend.

Mobile PCs können typischerweise sowohl mobil als auch stationär genutzt werden und damit auch auf unterschiedliche Netze zugreifen. Daraus resultiert, dass bei der mobilen Nutzung die Daten auf dem mobilen PC gegen Verlust, Manipulation und unberechtigte Einsichtnahme geschützt werden müssen. Andererseits muss sichergestellt werden, dass keine Gefährdungen von mobilen PCs auf andere IT-Systeme und Netze ausgehen können.

Bei der Nutzung von mobilen PCs durch verschiedene Personen muss die Übergabe geregelt stattfinden. Dabei muss mindestens nachvollziehbar sein, wo sich das Gerät befindet und welche Person das Gerät benutzt. Es ist eine Benutzerkennung anzustreben.

Datenträger

Alle Datenträger sind soweit möglich eindeutig zu kennzeichnen. Aus der Beschriftung soll die Verwendung (Verfahren, Dateien, Inhalt), Datum der ersten Ingebrauchnahme sowie das Datum des erstmaligen und letztmaligen Beschreibens hervorgehen. In der zuständigen Stelle ist ein Verzeichnis aller verwendeten Datenträger zu führen. Dieses Verzeichnis muss stets aktuell gehalten werden.

Die Weitergabe von Datenträgern darf nur an befugte Personen erfolgen. Befugt ist eine Person dann, wenn die Weitergabe der Datenträger im Verfahren vorgesehen ist. Die Weitergabe vertraulicher oder personenbezogener Daten auf Datenträgern darf nur gegen Quittung und datenschutzkonform erfolgen.

Wenn Datenträger, auf denen schützenswerte Daten gespeichert sind, zur weiteren Verwendung an Dritte gehen, müssen alle Daten vor der Weitergabe physisch gelöscht werden. Das kann mit geeigneten Programmen oder mit einem Gerät zum magnetischen Durchflutungslöschen erfolgen. Die von den Betriebssystemen dafür vorgesehenen Programme genügen in der Regel nicht. Eine Weitergabe an schulfremde Personen ist untersagt.

Auszusondernde oder defekte Datenträger müssen, sofern sie personenbezogene oder vertrauliche Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden. Vorzugsweise sind auch hier das Durchflutungslöschen und die mechanische Zerstörung anzuwenden.

Bei der Vergabe dieser Aufgaben an externe Dienstleister sind neben der gebotenen Sorgfalt bei der Auswahl des Auftragnehmers auch die übrigen Bestimmungen über Auftragsverarbeitung zu beachten.

Die Reparatur beschädigter Datenträger, auf denen schützenswerte Daten gespeichert sind, ist nur in besonderen Ausnahmenfällen erlaubt. Wenn unter besonderen Umständen Datenträger durch externe Dienstleister repariert werden sollen, ist der Auftragnehmer auf die Wahrung der Vertraulichkeit der Daten zu verpflichten. Die Verpflichtung muss vertraglich verankert sein.

Papiere mit vertraulichem Inhalt sind mit Hilfe eines Aktenvernichters zu vernichten. Bei der Beschaffung eines Aktenvernichters gelten dabei nach Angaben des TÜV Süd die Sicher­heits­stufen nach DIN 66399. Alternativ kann die Entsorgung auch über einen Dienstleister erfolgen. In diesem Fall muss sichergestellt sein, dass der Auftragnehmer über entsprechende Zertifikate verfügt. Der Auftragnehmer ist zur Protokollierung der Aktenvernichtung zu verpflichten.

#### Administration

Eine zuverlässige und sichere Erfüllung der IT-Aufgaben erfordert eine angemessene Personalausstattung, insbesondere in Hinblick auf die Sicherstellung eines kontinuierlichen Betriebs und der entsprechenden Vertretungsregelungen. Dabei spielen System- und Netzwerkadministratoren eine besondere Rolle.

Mit Administrationsaufgaben auf Netzwerk- und Systemebene dürfen nur ausgewählte, ausreichend qualifizierte, vertrauenswürdige und motivierte Mitarbeiter betraut werden.

Die Arbeit der Systemadministration ist durch eine spezielle Dienstanweisung geregelt.

Jegliche administrativen Berechtigungen bzw. Zugänge sind in einem administrativen Berechtigungskonzept festgelegt.

Administratives Personal wird vor Aufnahme derartiger Tätigkeiten gesondert geschult.

Die von den jeweiligen Systemen und der eingesetzten Software zur Verfügung gestellten administrativen Protokollierungsfunktionen werden genutzt. Zusätzlich wird jede admini­strative Änderung an Verfahren oder Systemen in der jeweiligen Verfahrensakte bzw. Systemakte festgehalten.

Durch einen geregelten Beauftragungsprozess wird Art und Umfang der Fern­wartungs­tätigkeiten vor Durchführung definiert, während der Durchführung vom Dienstleister doku­men­­tiert und nach der Durchführung geprüft und freigegeben.

Für alle Betreuungs- und Administrationsfunktionen sind Vertretungsregelungen erforderlich. Die Vertreter müssen alle notwendigen Tätigkeiten ausreichend beherrschen und ggf. auf schriftliche Arbeitsanweisungen und Dokumentationen zurückgreifen können. Die Vertre­tungs­regelung muss im System abgebildet sein und darf nicht durch die Weitergabe von Passwörtern erfolgen.

Die technischen Voraussetzungen für die Wahrnehmung einer Vertretung sollten möglichst ständig eingerichtet sein. Dort soll der Vertreter nur im Bedarfsfall auf das an geeigneter Stelle hinterlegte Passwort des Administrators zurückgreifen können.

Bei der Auswahl der Vertreter ist zu beachten, dass die Rollentrennung nicht unterlaufen wird.

Das Verwenden von Benutzerkennungen mit weitreichenden Administrationsrechten muss auf die dafür notwendigen Aufgaben beschränkt bleiben.

Die Administratoren erhalten für diese Aufgaben eine persönliche Administratorkennung. Für die alltägliche Arbeit sind Standard-Benutzerkennungen zu verwenden.

Die Administratoren sind durch organisatorische Regelungen (Dienstanweisungen o.ä.) je nach Schutzbedarf des Verfahrens bzw. der zu verarbeitenden Daten zu verpflichten, die im Rahmen ihrer Aufgaben durchgeführten Tätigkeiten zu protokollieren.

#### Notfallvorsorge

##### Notfallplan

Bei der Einführung neuer IT-Verfahren bzw. neuer IT-Arbeitsprozesse werden im Rahmen der Dokumentationspflichten Analysen zur Ermittlung des Schutzbedarfs und ggf. zur Identifizierung und Begegnung spezifischer Risiken vorgenommen. Basierend auf den Ergebnissen dieser Analysen sollte ein Notfallplan erstellt werden, in dem festgelegt wird, wie auf Notfallsituationen adäquat reagiert wird.

„Notfall“ bezeichnet eine Situation, in der durch eine Störung die Verfügbarkeit, Integrität oder Vertraulichkeit der Daten nicht mehr gegeben ist und ein verhältnismäßig hoher Schaden entsteht.

In einem Notfallplan sollten zum Beispiel Regelungen zu Verantwortlichkeiten, zum Wiederanlauf von IT-Systemen, zur Wiederherstellung von Daten und zum Einsatz von Ausweichmöglichkeiten enthalten sein.

Darüber hinaus ist es häufig sinnvoll einen Alarmierungsplan zu erstellen, in dem die Meldewege im Notfall beschrieben sind.

Maßnahmen zur Ausfallsicherheit sind entsprechend der jeweiligen Anforderung an die Verfügbarkeit zu ergreifen. IT-Systeme, die zur Aufrechterhaltung eines geordneten Betriebs notwendig sind, müssen durch Ausweichlösungen (redundante Geräteauslegung oder Übernahme durch gleichartige Geräte) oder Wartungsverträge mit kurzen Reaktionszeiten

hinreichend verfügbar gehalten werden.

##### Datensicherung

Die im Notfallplan enthaltene Erforderlichkeit einer Datensicherung muss nach einem dokumentierten Datensicherungskonzept erfolgen, das dem Schutzbedarf der zu sichernden Daten angemessen ist. Es muss auch darüber Auskunft geben, nach welchen Kriterien die Datensicherung der Daten erfolgt. Im Falle personenbezogener Daten sind die geforderten Mindest- bzw. Höchstzeiträume zu beachten.

Das Datensicherungskonzept umfasst alle Regelungen der Datensicherung (was wird von wem nach welcher Methode, wann, wie oft und wo gesichert). Ebenso ist die Aufbewahrung der Sicherungsmedien zu regeln. Alle Sicherungen und das Aufbewahren von Sicherungsmedien sind zu dokumentieren. (Datum, Art der Durchführung der Sicherung /gewählte Parameter, Beschriftung der Datenträger, Ort der Aufbewahrung)

Alle Anwender, die prinzipiell Datensicherungssysteme nutzen können, sollten über die Regelung zur Datensicherung informiert sein, um ggf. auf Unzulänglichkeiten (z.B. ungeeignetes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können.

Die Daten werden auf einem zentralen Fileserver gespeichert. Dort erfolgt turnusmäßig eine zentrale Datensicherung.

Die Sicherung der Daten auf Servern erfolgt täglich. Auch System- und Programmdaten sind nach Veränderungen zu sichern. Zur Datensicherung sind dafür geeignete Backup-Werkzeuge zu verwenden, die eine Datensicherung für Daten, deren Wiederherstellung mehr als einige Tage erfordert, nach dem Generationenprinzip unterstützen.

Nach Möglichkeit sind die Konfigurationen aller aktiven Netzkomponenten in eine regelmäßige Datensicherung einzubeziehen.

Die Konsistenz der Datensicherungsläufe ist sicher zu stellen, d.h. die Lesbarkeit der Datensicherung ist zu überprüfen. Das testweise Wiedereinspielen von Datensicherungen soll wenigstens einmal jährlich erfolgen.

Die Sicherungsdatenträger sind getrennt vom jeweiligen Rechner in einem anderen Gebäude aufzubewahren.

##### Benutzer

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass der zuständige IT-Verantwortliche bzw. Verfahrensverantwortliche rechtzeitig über das Ausscheiden oder den Wechsel eines Benutzers informiert wird.

Es sind sämtliche für den Ausscheidenden eingerichtete Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen.

## Restrisikoanalyse und Abhilfemaßnahmen

*Eine Restrisikoanalyse ist schulindividuell durchzuführen. Abhilfemaßnahmen sind zu entwickeln. Beispiele:*

Da aus Platzmangel einige der Großkopierer nicht in gesonderten Räumen untergebracht sind, besteht die Gefahr des unbefugten Zugriffes durch dritte Personen. Durch automatische Sperren des Bedienfeldes werden die Zugriffsmöglichkeiten zumindest stark eingeschränkt. Die Beschäftigten sind per Dienstanweisung verpflichtet, Ausdrucke mit personenbezogenen Daten auf Großkopierern sofort nach Beendigung des Ausdrucks zu entfernen und den Start des Ausdrucks durch Angabe eines PIN-Codes freizugegeben.

Durch menschliches Fehlversagen der Administratoren kann es zu Sicherheitsproblemen kommen. Die aktuelle Ausgestaltung der am Markt erhältlichen IT-Technologie bietet keine Möglichkeiten, dieses Restrisiko zu minimieren. Durch fortlaufende Schulung der Mitarbeiter wird einer unwissentlichen Fehlbedienung entgegengewirkt.

Die vor dem Serverraum angebrachten Schutzgitter sind für Einbrecher mit geringem Körpermaß und –umfang zu überwinden. Eine Alarmanlage erkennt jedoch diese Art von Einbruchsversuchen zuverlässig.

Die Serverraum-Wände und Türen entsprechen nicht den gültigen Schutzklassen. Durch Gewalteinwirkung kann sowohl die Tür als auch die Wand zum Serverraum aufgebrochen werden. Bauliche Änderungen sind nicht mit vertretbarem Aufwand durchführbar. Jedoch werden Einbruchsversuche außerhalb der Öffnungszeiten der Gemeindeverwaltung durch eine Alarmanlage zuverlässig erkannt.

Da sich im Serverraum ein Heizkörper befindet, besteht die Gefahr eines Rohrbruches. Aus diesem Grund stehen alle Server auf einer ca. 30cm hohen Plattform, um Schäden durch Wasser zu vermeiden.

Durch den Ausfall der Klimaanlage kann es zu einer Überhitzung des Serverraumes kommen. Die endgültige Lösung zur Temperaturüberwachung - mit rechtzeitiger Alarmierung des Hausmeisters und der Systemadministratoren - wird zurzeit noch diskutiert.

# Allgemeines

## Datenschutzerklärung Internet / Datenschutz-policy

Gegenstand des Datenschutzes sind personenbezogene Daten. Nach Art. 4 Abs.1 Nr 1 DSGVO sind dies alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Hierunter fallen z. B. Angaben wie Name, Post-Adresse, E-Mail-Adresse oder Telefonnummer, ggf. aber auch Nutzungsdaten wie die IP-Adresse.

Umfang der Datenverarbeitung

Wir beachten die Grundsätze der Datenverarbeitung, wie personenbezogene Daten verarbeitet werden müssen (Art. 5 Abs. 1 lit. a-f DSGVO).

Eine Weiter­­gabe Ihrer persönlichen Daten an Dritte erfolgt ohne ausdrückliche Einwilligung nicht, sofern dies nicht zur Erbringung der Dienstleistung, zur Vertrags­durchführung oder gesetzlich vorgeschrieben notwendig ist. Auch die Übermittlung an auskunftsberechtigte staatliche Institution und Behörden erfolgt nur im Rahmen der gesetzlichen Auskunfts­pflichten oder wenn wir durch eine gerichtliche Entscheidung zur Auskunft ver­pflichtet werden.

Auch den schulinternen Datenschutz nehmen wir sehr ernst. Unsere Mitarbeiter und die von uns beauftragten Dienstleistungsunternehmen sind von uns zur Verschwiegenheit und zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet worden.

Betroffene erhalten jederzeit ohne Angabe von Gründen kostenfrei Auskunft über die über sie bei uns gespeicherten Daten. Die Betroffenen können jederzeit ihre bei uns erhobenen Daten sperren, berichtigen oder löschen lassen. Auch können die Betroffenen jederzeit die uns ggf. erteilte Einwilligung zur Datenerhebung und Verwendung ohne Angaben von Gründen widerrufen. Wir stehen den Betroffenen jederzeit gern für weitergehende Fragen zu unserem Hinweisen zum Datenschutz und zur Verarbeitung ihrer persönlichen Daten zur Verfügung.

## Übersicht Fachverfahren

Folgende Fachverfahren werden geführt:

**Schnittstellen Module:**

* IServ-Portalserver – Modul „Brockhaus-Integration“
* IServ-Portalserver – Modul „Drucken“
* IServ-Portalserver – Modul „Edupool“
* IServ-Portalserver – Modul „Fernwartung“
* IServ-Portalserver – Modul „Gerätebewerbung“
* IServ-Portalserver – Modul „Gruppenbewerbung“
* IServ-Portalserver – Modul „Import“
* IServ-Portalserver – Modul „Klausurmodus“
* IServ-Portalserver – Modul „Netzwerkmonitor“
* IServ-Portalserver – Modul „OAuth- und Open-ID-Connect-Server“
* IServ-Portalserver – Modul „Online-Medien“
* IServ-Portalserver – Modul „Pläne“
* IServ-Portalserver – Modul „Rechnersperre“
* IServ-Portalserver – Modul „Rechnersteuerung“
* IServ-Portalserver – Modul „Schulserver“
* IServ-Portalserver – Modul „Schülerkarriere“
* IServ-Portalserver – Modul „Softwareverteilung“
* IServ-Portalserver – Modul „Softwareverteilung Linux“
* IServ-Portalserver – Modul „Speicherplatzanzeige“
* IServ-Portalserver – Modul „Statistik“
* IServ-Portalserver – Modul „Stundenplan“
* IServ-Portalserver – Modul „Störungsmeldung Reese IT“
* IServ-Portalserver – Modul „Störungsmeldung Stadt Kiel“
* IServ-Portalserver – Modul „Systemmonitor“
* IServ-Portalserver – Modul „WebDAV“
* IServ-Portalserver – Modul „WLAN-Modul (RADIUS)“
* IServ-Portalserver – Modul „GIGATRADE Network GmbH Fernwartung“
* IServ-Portalserver – Modul „Jens Schönfelder Fernwartung“
* IServ-Portalserver – Modul „Kommunales Rechenzentrum Minden-Ravensberg/Lippe Fernwartung“
* IServ-Portalserver – Modul „Medienzentrum Osnabrück Fernwartung“
* IServ-Portalserver – Modul „osnaware Fernwartung“
* IServ-Portalserver – Modul „Phywe Fernwartung“
* IServ-Portalserver – Modul „Reese IT Fernwartung“
* IServ-Portalserver – Modul „IServ Schulfilter-Plus-Integration“
* IServ-Portalserver – Modul „TIME for kids Fernwartung“

**Eigenständige Module:**

* IServ-Portalserver – Modul „Aufgaben“
* IServ-Portalserver – Modul „Buchungen“
* IServ-Portalserver – Modul „Didaktische-methodische Planung“
* IServ-Portalserver – Modul „Forum“
* IServ-Portalserver – Modul „Infobildschirm“
* IServ-Portalserver – Modul „Kalender“
* IServ-Portalserver – Modul „Knowledge-Base“
* IServ-Portalserver – Modul „Kurswahlen“
* IServ-Portalserver – Modul „Messenger“
* IServ-Portalserver – Modul „Mobilgeräteverwaltung“
* IServ-Portalserver – Modul „News“
* IServ-Portalserver – Modul „Videokonferenz
* IServ-Portalserver – Modul „Office“
* IServ-Portalserver – Modul „Schnellumfragen“
* IServ-Portalserver – Modul „Störungsmeldung“
* IServ-Portalserver – Modul „Texte“
* IServ-Portalserver – Modul „Umfragen“
* IServ-Portalserver – Modul „Webfilter“
* IServ-Portalserver – Modul „Webfilter SafeSearch“
* IServ-Portalserver – Modul „Klausurplan“
* IServ-Portalserver – Modul „Wartungsarbeiten für IServ“
* IServ-Portalserver – Modul „IServ Modul für Gruppenlisten“
* IServ-Portalserver – Modul „Mediotheksmodul für IServ“
* IServ-Portalserver – Modul „Die Schulbuchausleihe für IServ“
* IServ-Portalserver – Modul „osnaware Vokabeltrainer für IServ“
* IServ-Portalserver – Modul „Phywe ExperimentierManager“
* IServ-Portalserver – Modul „TIME for kids Schulfilter Plus“

## Verträge (Kauf, Wartung Auftragsverarbeitung)

Die Verarbeitung von Daten im Auftrag oder auch die Wartung von IT-Systemen oder -An­wendungen durch Dritte kann ein Risiko für die Sicherheit der Daten darstellen. Eine schriftliche Vereinbarung ist Voraussetzung für alle im Auftrag dieser Schule betriebenen IT-Verfahren. Es ist eine eindeutige Zuweisung der Verantwortlichkeit für die IT-Sicherheit zu schaffen und entsprechende Kontrollmöglichkeiten vorzusehen. Es sind die entsprechenden Regelungen der DSGVO zu beachten.

Folgende Fälle der Auftragsverarbeitung liegen aktuell vor:

|  |  |  |  |
| --- | --- | --- | --- |
| Zweck | Auftragnehmer | AV-Vertrag vom | Ablageort |
| IT–Systembetreuung für Hardware und Software für den „IServ-Portalserver“ | IServ GmbH, Bültenweg 73, 38106 Braunschweig |  |  |
|  |  |  |  |

*Die Liste muss ggfs. schulindividuell ergänzt werden.*

Teil dieser Verträge muss immer die Darstellung der technischen und organisatorischen Maßnahmen sein, die der Auftragsverarbeiter beilegen muss. Ebenso sind eventuelle Unter-Auftragsverarbeiter aufzulisten.

## Aus- und Fortbildung

Das IT-Personal darf erst nach ausreichender Schulung mit IT-Verfahren arbeiten. Dabei sind ihnen die für sie geltenden Sicherheitsmaßnahmen, die rechtlichen Rahmenbedingungen sowie ggf. die Erfordernisse des Datenschutzes zu erläutern. Es muss sichergestellt sein, dass die ständige Fortbildung des IT-Personals in allen ihr Aufgaben­gebiet betreffenden Belangen erfolgt. Hier ist in diesem Rahmen besonders auf die IServ-Admin-Schulungen hinzuweisen.

## Dienstanweisungen (allgemein und bezüglich Internet)

Die aktuellen Dienstanweisungen sind abgelegt unter:

## Datenschutz- und Sicherheitsmanagement

### Datenschutzbeauftragter

*Als behördlicher Datenschutzbeauftragter ist … bestellt.*

### Regelmäßige Kontrollen

Im Rahmen von regelmäßigen Kontrollen wird die Vollständigkeit der Verfahrens- und Systemdokumentation geprüft. Einmal jährlich werden sämtliche Systemakten und Verfahrensakten auf Vollständigkeit und Aktualität geprüft. Sämtliche Verträge zur Auftragsverarbeitung werden zumindest jährlich auf korrekte Darstellung des Vertrags­gegenstands und insbesondere auf eine ausreichende Dokumentation der zu treffenden Weisungen und Regelungen zur Verarbeitung personenbezogener Daten geprüft. Die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen, die in diesem Konzept festgelegt sind, werden mindestens einmal jährlich überprüft.

### Anlassbezogene Kontrollen

Ergeben sich durch Berichterstattung in der Fachpresse, aufgrund von Meldungen der Soft­warehersteller oder aus anderen Publikationen Hinweise, dass diese Schule ihre Sicher­heits­konzeption neu prüfen muss, so wird der Datenschutzbeauftragte in Zusammenarbeit mit der Administration eine entsprechende Prüfung durchführen. Eine solche Prüfung kann auch nachfolgend zu einem Sicherheitsvorfall durchgeführt werden.

Die Ergebnisse dieser Kontrollen werden durch den Datenschutzbeauftragten dokumentiert.

### Verhalten bei Sicherheitsvorfällen

Ein Sicherheitsvorfall ist ein Schadensereignis unter Verstoß gegen die Sicherheitsziele bzw. die in diesem Dokument festgelegten Sicherheitsmaßnahmen.

Sollte es zu einem Sicherheitsvorfall kommen, so werden durch ein geordnetes, vorab festgelegtes Vorgehen eine korrekte und schnelle Behebung des Vorfalls sowie eine strukturierte Nachbereitung gewährleistet.

Sicherheitsvorfälle werden in einem zweistufigen Verfahren bearbeitet.

In der ersten Stufe hat die Behebung des Sicherheitsvorfalls und die Information der möglicherweise Betroffenen absolute Priorität. Der Datenschutzbeauftragte benachrichtigt zunächst die Schulleitung dieser Schule.

Im Folgenden koordiniert der Datenschutzbeauftragte die Bearbeitung des Sicherheitsvorfalls und trifft die notwendigen Maßnahmen zur Behebung.

Für Zwecke der späteren Nachbereitung müssen alle mit dem Sicherheitsvorfall ver­bun­denen Vorgänge und Entscheidungen nachvollziehbar dokumentiert werden. Zur Bear­beitung von Sicherheitsvorfällen sind außerdem technische Unterlagen wie Protokolle oder für den Vorfall besonders relevante System-Meldungen zu speichern und zu archivieren. Die Regelungen des Datenschutzes müssen auch bei der Bearbeitung von Sicherheitsvorfällen eingehalten werden. Der Datenschutzbeauftragte ist verantwortlich für die Dokumentation.

In der zweiten Stufe muss der Sicherheitsvorfall nachbereitet werden. In einem Bericht bewertet der Datenschutzbeauftragte die bereits dokumentierten Vorgänge, Entscheidungen und Maßnahmen. Der Bericht soll darüber hinaus ermöglichen, Verbesserungen an den Notfallstrategien vorzunehmen und bekannte Fehler zu vermeiden.

### Integration von Datenschutz und Datensicherheit

Der Datenschutzbeauftragte ist bei jeder Beschaffung von Informations- und Kommu­nikationstechnologie zu beteiligen.

Bei der Planung neuer Verfahren oder wesentlicher Änderung der Informations- und Kommu­nikationstechnologie nimmt der Datenschutzbeauftragte Stellung. Er ist frühzeitig zu beteiligen.