Leitlinie zur Informationssicherheit Sekundarschule Hausen am Albis, Kappel am Albis und Rifferswil

Änderungskontrolle

Version	Datum	Beschreibung, Bemerkung	Name
1.1	30.03.2025	Grundlagendokument erstellt	B. Moser & S. Zemp
1.2	27.04.2025	Vernehmlassung SPF	SPF

1 Einleitung

Die Sekundarschule Hausen am Albis, Kappel am Albis und Rifferswil (Sek Hausen) ist zur Aufgabenerfüllung von zuverlässig funktionierenden Systemen der Informations- und Kommunikationstechnologie abhängig. Zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit und Authentizität der Informationen und deren Verarbeitungssysteme nach § 7 Gesetz über die Information und den Datenschutz (IDG, LS 170.4) verabschiedet die Schulpflege diese Leitlinie zur Informationssicherheit. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Sek Hausen angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet die Leitlinie eine Beschreibung der Informationssicherheitsorganisation.

2 Geltungsbereich

Die Leitlinie zur Informationssicherheit und die damit zusammenhängenden Dokumente gelten für alle Mitarbeitenden der Sek Hausen sowie für Behördenmitglieder. Vertragspartner, die Daten bearbeiten, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet.

3 Informationssicherheitsniveau

Die Schulpflege der Sek Hausen hat entschieden, dass ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf angestrebt werden soll. Für Datensammlungen mit einem höheren Schutzbedarf werden zusätzliche Sicherheitsmassnahmen getroffen.

4 Informationssicherheitsziele

Aus der Einstufung ergeben sich die folgenden Informationssicherheitsziele (§ 7 IDG):

Integrität	Informationen müssen richtig und vollständig sein.
Nachvollziehbarkeit	Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
Verantwortung	Die politischen Behörden und die Mitarbeitenden der Schule sind sich ihrer Verantwortung beim Umgang mit Informationen, IKT-Systemen[1] und Anwendungen bewusst. Sowohl Behörde als auch Mitarbeitende unterstützen die Informationssicherheitsziele.
Verfügbarkeit	Informationen müssen bei Bedarf vorhanden sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Schul- und Verwaltungsbetrieb haben.
Vertraulichkeit	Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.
Zurechenbarkeit	Informationsbearbeitungen müssen einer Person zugerechnet werden können.

[1] Informations- und Kommunikationstechnologien (IKT) umfasst alle technischen Medien, die für die Handhabung von Informationen und zur Unterstützung der Kommunikation eingesetzt werden; hierzu zählen unter andere, Computer- und Netzwerkhardware sowie die zugehörige Software.

5 Informationssicherheitsmassnahmen

Die Auswahl der technischen und organisatorischen Massnahmen erfolgt anhand der Anforderungen der ISO/IEC 27001 und den IKT-Minimalstandards des Bundesamts für Cybersicherheit (BACS):

Aktualisierungen (Updates)	Alle IKT-Systeme (Server, Clients und Netzwerkkomponenten) werden regelmässig aktualisiert und mit den neusten Sicherheitsupdates versorgt.
Archivierung / Löschung	Alle Daten werden gemäss den regulatorischen Vorgaben archiviert. Falls eine Aufbewahrung nicht mehr erforderlich ist, werden diese sicher gelöscht.
Berechtigungskonzept	Der Zugriff auf die Informationen ist durch ein Berechtigungskonzept geregelt. Die Zugriffsberechtigungen der Behördenmitglieder, der Mitarbeitenden sowie der Lernenden auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben erforderlich und geeignet.
Datenschutz	Alle Daten werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet. Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen.
Datensicherung (Backup)	Die Datensicherung wird regelmässig durchgeführt. Die Sicherungsmedien werden an getrennten Orten aufbewahrt und sind physisch geschützt. Es wird gewährleistet, dass verlorene oder fehlerhafte Teile des Informationsbestands über eine ausreichende Dauer wiederhergestellt werden können.
IKT-Systeme	Die IKT-Systeme werden nach der Beschaffung sicher installiert (gemäss anerkannten Sicherheitsstandards) und betrieben, mit einem Änderungsmanagement verwaltet und in einem geregelten Prozess ausser Betrieb genommen.
Mobile Geräte / Software	Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten inklusive der Verwendung von privaten Geräten (Bring Your Own Device) sowie der Installation von Software auf Arbeitsplatzrechnern und Servern werden im Detail geregelt. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.
Überwachung (Monitoring)	Die Verfügbarkeit und Qualität der Anwendungsdienste werden laufend überprüft.
Netzwerk / Firewall	Alle Netzwerkzugänge werden gesichert. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern. Die vom Kanton vorgegebene Network Security Policy der übergeordneten Netzwerke (Leunet) wird eingehalten.
Organisation	Die relevanten Funktionen der Organisation sind festgelegt und in einem Organigramm dokumentiert. Für alle Funktionen ist die Stellvertretung geregelt. Durch ausreichende Dokumentation und Instruktion wird sichergestellt, dass die Stellvertretenden ihre Aufgabe erfüllen können.

Outsourcing	Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart werden.
Passwörter	Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch mitarbeiterabhängige Passwörter gesichert. Es wird eine ausreichende Qualität der Passwörter sichergestellt.
Sensibilisierung / Schulung	Die Mitarbeiterinnen und Mitarbeiter nehmen mindestens jährlich an einer internen Sicherheitsschulung der für die Informationssicherheit verantwortlichen Person teil. Sie werden regelmässig über aktuelle Gefahren und zu treffende Massnahmen informiert.
Verschlüsselung	Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, beispielsweise besondere Personendaten, erfolgt verschlüsselt über öffentliche Netze.
Virenschutz / Internet	Virenschutzprogramme werden auf allen IKT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.
Weisungen	Die Mitarbeiterinnen und Mitarbeiter werden angewiesen, die Gesetze sowie die vertraglichen Regelungen und internen Richtlinien einzuhalten. Sie unterstützen durch eine sicherheitsbewusste Arbeitsweise die Sicherheitsmassnahmen. Informationssicherheitsfragen und Hinweise auf Schwachstellen werden an die für die Informationssicherheit verantwortliche Person gerichtet.
Zutritt	Gebäude und Räume sowie IKT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt.
Physische Sicherheit	Brandschutzmassnahmen, Zutrittskontrolle usw.

6 Informationssicherheitsorganisation

Die Schulpflege, die für die Informationssicherheit verantwortliche Person (ISV) und die für die einzelnen Bereiche zuständigen Daten- und Anwendungsverantwortlichen haben die zentralen Rollen in der Informationssicherheitsorganisation inne.

Die Informationssicherheitsorganisation ermöglicht es der Sek Hausen, das angestrebte Informationssicherheitsniveau zu erreichen und dieses aufrechtzuerhalten. Informierte und geschulte Mitarbeitende sind die Voraussetzung dafür, dass die Sek Hausen die gesteckten Informationssicherheitsziele erreichen kann. Auf ihre Sensibilisierung und Weiterbildung ist besonderes Gewicht zu legen.

Schulpflege

Die Schulpflege trägt die Gesamtverantwortung für die Informationssicherheit in der Sek Hausen. Sie legt die Leitlinie zur Informationssicherheit fest und genehmigt die für die Informationssicherheit erforderlichen Massnahmen und Mittel. Sie weist die Rolle/Funktion Informationssicherheitsverantwortliche/Informationssicherheitsverantwortlicher (ISV) und Datenschutzberaterin/Datenschutzberater je einer verantwortlichen Person zu.

Informationssicherheitsverantwortliche/Informationssicherheitsverantwortlicher
Die/der ISV ist zur Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus und für die Informationssicherheit verantwortlich. Sie/er ist für die Ausarbeitung und Nachführung eines Sicherheitskonzepts verantwortlich und berichtet in dieser Funktion direkt der Schulpflege.

Der oder dem ISV werden ausreichende finanzielle und zeitliche Ressourcen für die Ausübung ihrer/seiner Tätigkeit zur Verfügung gestellt. Die Daten- und Anwendungsverantwortlichen sowie die IKT-Benutzerinnen und Benutzer unterstützen sie/ihn in ihrer/seiner Tätigkeit. Sie/er wird in alle Projekte, die IKT betreffen, involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.

Für sicherheitsrelevante Fragen ist die/der ISV weisungsberechtigt. Sie/er ist die Anlaufstelle für Informationssicherheitsfragen und Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

Datenschutzberaterin/Datenschutzberater
Der Datenschutz und die Informationssicherheit sind für alle Bereiche, in denen personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Zur Umsetzung des Datenschutzes ist die Datenschutzberaterin/der Datenschutzberater verantwortlich. Sie/er arbeitet in dieser Rolle eng mit der/dem ISV zusammen und ist Ansprechperson bei Datenschutzfragen.

Anwendungs- und Datenverantwortliche
Für alle Prozesse, Daten, Anwendungen, IKT- und Netzwerksysteme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf (Klassifizierung) bestimmt und die Zugriffsberechtigungen vergibt.

7 Kontinuierliche Verbesserung der Informationssicherheit

Die Schulpflege unterstützt die Einhaltung und fortlaufende Verbesserung des Informationssicherheitsniveaus. Sie gibt mit der periodischen Überarbeitung dieser Leitlinie zur Informationssicherheit die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung. Die Leitlinie wird alle 2 Jahre überprüft.

Das Informationssicherheitskonzept und deren Umsetzung wird alle 2 Jahre sowie zusätzlich bei Projekten mit grossen Auswirkungen auf den Datenschutz und Informationssicherheit auf Aktualität und Wirksamkeit geprüft. Festgestellte Abweichungen werden innert nützlicher Frist behoben.

Die zu ergreifenden Massnahmen orientieren sich am Stand der Technik sowie an nationalen und internationalen Standards.

Beschlossen von der Schulpflege mit Beschluss [Nr.] am [Datum].

Esther Flückiger
Schulpräsidentin

Barbara Moser
Ressort Informatik und Kommunikation