Kantonsschule Ausserschwyz

SRKSA 600.10

Weisungen über die

IT-Sicherheit

an der Kantonsschule Ausserschwyz

Inhaltsverzeichnis

1. Unsere schulische Verantwortung

Mit der vorliegenden Sicherheitspolitik, die für alle Mitarbeitenden und Lernenden der KSA verbindlich ist, werden wir unserem Ruf als moderne und verantwortungsvolle Schule gerecht. Sie regelt den Umgang mit den Daten und den IT-Systemen.

Oberstes Prinzip der IT-Sicherheit für unsere Mitarbeitenden und Lernenden ist die hohe Verfügbarkeit unserer IT-Systeme. Unser Berufsethos schliesst das Prinzip Vertraulichkeit in unsere schulische Verantwortung ein.

Unsere Mitarbeitenden und Lernenden haben ein Recht darauf, dass wir keine Personendaten ohne Einwilligung der betroffenen Personen weitergeben.

2. Unsere Schutzobjekte

Für elektronische Informationen gilt der Grundsatz, dass sie mindestens so gut geschützt werden wie schützenswerte Daten auf Papier.

In unserem Fall trifft dies auf alle Informationen zu, welche Mitarbeitende oder Lernende auf unseren Servern ablegen. Wir unterscheiden dabei Informationen, welche auf dem Administrationsnetz abgelegt werden, und Informationen, welche auf dem Schulnetz abgelegt werden.

Als Schule, welche ihre Systeme und Daten via Internet allen Mitarbeitenden und Lernenden zugänglich macht, kommt dem Faktor Sicherheit und Vertrauenswürdigkeit eine besondere Bedeutung zu.

Als „Informationssysteme“ bezeichnen wir die Gesamtheit von Hardware, Software und Daten sowie von Kommunikations- und manuellen Vorgängen, die ein zusammenhängendes System zur Informationsverarbeitung bzw. zur Informationsanwendung ausmachen. Dabei ist es unerheblich, ob die Verarbeitung manuell oder rechnergestützt erfolgt.

„Informationsinfrastruktur“ umfasst alle Örtlichkeiten und Einrichtungen zur Unterbringung, zur Erschliessung und zum Betrieb unserer Informationssysteme wie zum Beispiel Gebäude, Räume, Antennen und die Verkabelung für Energieversorgung und Netzwerke.

3. Schutzziele, Schutzgrad, Qualitätssicherung

Wir schützen unsere Objekte nach technischen und organisatorischen Gesichtspunkten bestmöglich im Rahmen unserer zugesprochenen Ressourcen. Diese Sichtweise ist einer dauernden Prüfung und Anpassung zu unterziehen.

Beim Umgang mit unseren Schutzobjekten beachten wir immer die folgende Rangfolge unserer Schutzziele:

1. **Vertraulichkeit aller Personendaten**
2. **Integrität aller Personendaten**
3. **Verfügbarkeit der Informations-Systeme**
4. **Umsetzen von Neuerungen**

Die Grundschutzmassnahmen gelten für alle unsere Schutzobjekte ohne Unterschied. Zusätzliche Schutzgrade für spezifische Systeme, resp. Anforderungen werden separat definiert. Dabei leiten wir angemessene und branchenübliche Massnahmen ab, wenn erhöhte Schutzziele zu beachten sind.

Es ist klar definiert, wer die Verantwortung für Beschaffung, Betrieb, Unterhalt und Entsorgung der Schutzobjekte trägt. Für Notfälle gibt es eine Notfallplanung.

Alle diese Anordnungen und Massnahmen beschränken die Gefahren der unbeabsichtigten / regelwidrigen Informationsverarbeitung auf ein tolerierbares und zahlbares Restrisiko. Bewusst eingegangene Risiken werden dokumentiert und durch die Schulleitung genehmigt.

Wir wenden die Grundsätze der Qualitätssicherung auf alle unsere Schutzobjekte und Arbeiten an. Alle gesetzlichen, vertraglichen und internen Vorgaben werden strikt befolgt.

4. Vertraulichkeit und Vertrauenswürdigkeit

4.1. Speicherplatz für Daten

Die Schule unterscheidet zwischen vertrauenswürdigen und öffentlichen Daten.

Als vertrauenswürdigen Daten werden bezeichnet: Personendaten und organisatorische, resp. verwaltungsspezifische Daten.

Alle vertrauenswürdigen Daten müssen auf dem Administrationsnetz gespeichert werden oder in dem für diese Zwecke vorgesehenen Teil des Intranets. Auf dieses Netz haben nur Schulleitungsmitglieder und Verwaltungsangestellte Zugriff.

4.2. Verantwortung

Die Schulleitung bezeichnet die vertrauenswürdigen Daten. Sie garantiert für die Richtigkeit, Aktualität und Vollständigkeit dieser Daten und regelt die Zugriffskontrolle. Werden persönliche Daten herausgegeben, so darf das nur im Rahmen des Datenschutzgesetzes geschehen. Die Schulleitung regelt auch den Umgang mit veralteten, resp. archivierten Daten.

4.3. Zugriffskontrolle

Alle unsere Schutzobjekte werden durch den vom Schulrechenzentrum Ausserschwyz (SRZA)-Betreiber bezeichneten Administrator verwaltet, damit die Sicherheit und die Zugriffskontrolle zu den Daten gewährleistet sind.

4.4. Vertrauenswürdige Informationssysteme

Unsere Informationssysteme sind vertrauenswürdig und erzwingen auf technisch effektive Weise die Vertraulichkeit.

4.5. Datensicherheit und Datensicherung

Auf alle unsere Systeme und Daten darf nur gesichert zugegriffen werden, d.h. verschlüsselt. Es gibt keinen ungesicherten Hintereingang, Ausnahme Remotezugriff SRZA für Wartungen. Beim zentralen Firewall werden alle unnötigen Ports geschlossen. Der zentrale Firewall trennt das Administrationsnetz vom Schulnetz. Der Zugriff vom Administrations- auf das Schulnetz ist gewährleistet, umgekehrt aber nicht. Das öffentlich zugängliche Intranetportal befindet sich in einer Demilitarisierten Zone (DMZ), d.h. nur der zivilen Nutzung offen.

Das Datensicherungskonzept ist im Dokument «Interne Weisungen» festgelegt.

Alle Schutzobjekte müssen redundant gesichert werden.

4.6. Dokumentation der einzelnen Schutzobjekte

Alle Installationen werden dokumentiert und auf den Systemen des SRZA-Betreibers abgelegt. Alle Wartungsarbeiten werden ebenfalls elektronisch dokumentiert. Eine gedruckte Form der Installationen kann auf Verlangen im SRZA eingesehen werden.

5. Organisation

5.1. Schulleitung

Die Schulleitung legt die IT-Sicherheitspolitik fest und trägt die Gesamtverantwortung für die Umsetzung.

5.2. IT Security Manager

Die Aufgaben des IT Security Manager werden durch den Projektleiter des SRZA wahrgenommen. Er entwickelt in Zusammenarbeit mit der Rektorin der KSA das Informationssicherheitskonzept und leitet daraus die Weisungen zur Informationssicherheit ab, welche von der Schulleitung verbindlich erklärt werden. Er übernimmt das Projekt- und Betriebscontrolling.

Die Überprüfung und die permanente Aktualisierung der Angemessenheit unserer Massnahmen zur Informationssicherheit ist ein dauernder Prozess. Der IT Security Manager macht die Schulleitung auf nötige Anpassungen der Sicherheitspolitik aufmerksam.

5.3. Mitarbeitende und Lernende

Die Mitarbeitenden werden mit der Unterzeichnung der **„Benutzungsrichtlinien für den Umgang mit Informatikmitteln an der Kantonsschule Ausserschwyz“** verpflichtet, die Informationssicherheit zu wahren und die vorgegebenen Regeln einzuhalten.

Die Lernenden werden mit der Unterzeichnung der **„Benutzungsregeln für den "PC-Einsatz an der Kantonsschule Ausserschwyz“** verpflichtet, die Informationssicherheit zu wahren und die vorgegebenen Regeln einzuhalten.

Alle Mitarbeitenden erhalten eine standardisierte Einführung in die EDV an der KSA.

Bei Sicherheitsproblemen besteht für alle Mitarbeitenden und Lernenden eine persönliche Informationspflicht. Bei Nichteinhaltung der Regeln zur Informationssicherheit können privatrechtliche und arbeitsrechtliche Sanktionen ergriffen werden. Muss Schadenersatz geleistet werden, hat die KSA ein Regressrecht.

5.4. Informationstreuhänder

Lieferanten und Firmen für den Betrieb und die Wartung, insbesondere die Mitarbeiter des SRZA, nehmen als Informationstreuhänder ihre Aufgaben im Rahmen der mit ihnen vereinbarten Verträge wahr, welche den Umfang der Leistungen auf der Grundlage unserer Regelungen bestimmen.

6. Prüfverfahren und Kontrollen

Der IT Sicherheitsbeauftragte des Kantons ist zuständig für die Kontrolle der Informationssicherheit.

Der IT Security Manager führt jährlich prophylaktisch eine Kontrolle gemäss einer Checkliste durch, die vorher durch die Betriebskommission des SRZA genehmigt wird.

7. Inkraftsetzung und Änderung

Die Schulleitung hat die vorliegende IT-Sicherheitspolitik am 19. Oktober 2006 verabschiedet und in Kraft gesetzt.

Die Schulleitung

genehmigt an der Schulleitungssitzung vom 19. Oktober 2006.