Leitlinien zur Informationssicherheit an der Schule Zumikon

Inhaltsverzeichnis

JILL VANESSA IJSSELING

Digital signiert von JILL VANESSA IJSSELING
DN: cn=JILL VANESSA IJSSELING, c=CH
Datum: 2024.05.21 14:02:09 +02'00'

Verabschiedet von der Schulpflege Zumikon am 14. Mai 2024.

Inkrafttreten am 1. Juni 2024.

Sprachregelung
Nach Möglichkeit wird bei Funktions- und Rollenbezeichnungen eine geschlechtsneutrale Form verwendet.

1. Grundsätzliches

Art. 1 Einleitung

Die Schule Zumikon 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 Leitlinien zur Informationssicherheit. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Schule Zumikon angestrebte Informationssicherheitsniveau, die -ziele sowie die geeigneten Massnahmen definiert. Weiter beinhalten die Leitlinien eine Beschreibung der Informationssicherheitsorganisation.

Art. 2 Geltungsbereich

Die Leitlinien zur Informationssicherheit und die damit zusammenhängenden Dokumente (insbesondere das Rollen- und Berechtigungskonzept, das Sicherheitskonzept, die Informationssicherheitsorganisation und die Anleitung Sensibilisierung der Mitarbeitenden) gelten für alle Mitarbeitenden der Schule Zumikon. Vertragspartner, die Daten bearbeiten, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet.

2. Niveau der Informationssicherheit

Art. 3 Schutzstufe 1 Grundschutz

Das Informationssicherheitsniveau der Schule Zumikon entspricht der «Schutzstufe 1 – Grundschutz» gemäss Allgemeiner Informationssicherheitsrichtlinie AISR der kantonalen Verwaltung. Diese Einstufung erfolgt aufgrund der Tatsache, dass die Anzahl der betroffenen Personen gering ist, alle wesentlichen Funktionen und Aufgaben durch IT- und Netzwerksysteme unterstützt werden und ein Ausfall von IT- und Netzwerksystemen die Aufgabenerfüllung nicht länger beeinträchtigen darf. Die Schule Zumikon bearbeitet auch Daten, die eines erhöhten Schutzes bedürfen vor unberechtigten Zugriffen und unerlaubten Änderungen.

3. Ziele der Informationssicherheit

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

Art. 4 Integrität und Nachvollziehbarkeit

1. Informationen müssen richtig und vollständig sein.
2. Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.

Art. 5 Verantwortung

Die Mitarbeitenden der Schule sind sich ihrer Verantwortung beim Umgang mit Informationen, IT-Systemen und Anwendungen bewusst. Sie unterstützen die Informationssicherheitsziele.

Art. 6 Verfügbarkeit

Informationen müssen bei Bedarf vorhanden sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Schulbetrieb haben.

Art. 7 Vertraulichkeit

Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.

Art. 8 Zurechenbarkeit

Informationsbearbeitungen müssen einer Person zugerechnet werden können.

Art. 9 Aktualisierung/Update Archivierung / Löschung

1. Alle IT-Systeme (Server, Clients und Netzwerkkomponenten) werden regelmässig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.
2. Alle Daten werden gemäss den regulatorischen Vorgaben archiviert. Falls eine Aufbewahrung nicht mehr erforderlich ist, werden diese sicher gelöscht.

Art. 10 Berechtigungskonzept

Der Zugriff auf die Informationen ist durch ein Berechtigungskonzept geregelt. Die Zugriffsberechtigungen für die Behörde und alle Mitarbeitenden sowie für Lernende auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben geeignet und erforderlich.

Art. 11 Datenschutz und -sicherung (Back-up)

1. 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.
2. 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.

Art. 12 IT-Systeme

Die IT-Systeme werden nach der Beschaffung sicher installiert (gemäss anerkannter Sicherheitsstandards) und betrieben, mittels eines Änderungsmanagements verwaltet und in einem geregelten Prozess ausser Betrieb genommen.

Art. 13 Mobile Geräte / Software

Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten inklusive der Verwendung von privaten Geräten (Bring Your Own Device) sowie die Installation von Software auf Arbeitsplatzrechnern und Servern sind geregelt. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.

Art. 14 Monitoring / Überwachung

Die Verfügbarkeit und Qualität der Anwendungsdienste werden laufend überprüft.

Art. 15 Netzwerk / Firewalls

Alle Netzwerkzugänge werden gesichert. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern, u. a. auch die vom Kanton vorgegebene Network Security Policy der übergeordneten Netzwerke (LEUnet) wird eingehalten.

Art. 16 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 Aufgaben erfüllen können.

Art. 17 Outsourcing

Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Datensicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart werden.

Art. 18 Passwörter

Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch mitarbeiterabhängige Passwörter gesichert. Es wird eine ausreichende Qualität der Passwörter sichergestellt.

Art. 19 Sensibilisierung

Die Mitarbeiterinnen und Mitarbeiter sowie die Lernenden nehmen jährlich an einer internen Sicherheitsschulung der für die Informationssicherheit verantwortlichen Person teil. Sie werden regelmässig über aktuelle Gefahren und zu treffende Massnahmen informiert.

Art. 20 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.

Art. 21 Virenschutz

Virenschutzprogramme werden auf allen IT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Art. 22 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.

Art. 23 Zutritt / Physische Sicherheit

1. Gebäude und Räume sowie IT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt.

2. Es werden Sicherheitsmassnahmen wie Brandschutz usw. umgesetzt.

4. Organisation der Informationssicherheit

Art. 24 Verantwortlichkeiten und Sicherheitsniveau

1. Die Schulpflege Zumikon, der/die Informationssicherheitsverantwortliche und die für die einzelnen Bereiche zuständigen Daten- und Anwendungsverantwortlichen haben zentralen Rolle in der Informationssicherheitsorganisation inne.

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

3. Die Informationssicherheitsorganisation der Schule Zumikon ist im Anhang A – Organigramm der Schule Zumikon definiert.

Art. 25 Die Schulpflege

Die Schulpflege trägt die Gesamtverantwortung für die Informationssicherheit in der Schule Zumikon. Sie legt die Leitlinien zur Informationssicherheit fest und genehmigt die für die Informationssicherheit erforderlichen Mass-

nahmen und Mittel. Sie weist die Rolle / Funktion Informationssicherheitsverantwortliche / Informationssicherheitsverantwortlicher einer verantwortlichen Person zu.

Art. 26 Verantwortliche/r für die Informationssicherheit

1. Zur Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus wird durch die Schulpflege Zumikon eine Person bestimmt, die für die Informationssicherheit verantwortlich ist. Sie ist für die Ausarbeitung und Nachführung eines Sicherheitskonzepts verantwortlich und berichtet in dieser Funktion direkt der ihr oder ihm vorgesetzten Stelle.

2. Die IT- und Anwendungsverantwortlichen sowie die IT-Benutzerinnen und IT-Benutzer unterstützen sie / ihn in ihrer / seiner Tätigkeit. Sie / er wird in alle Projekte involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.

3. Über sicherheitsrelevante Fragen entscheidet die / der Informationssicherheitsverantwortliche und bemüht sich um entsprechende Ausnahmen. Die Person ist die Anlaufstelle für Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

4. Aufgaben der / des Informationssicherheitsverantwortlichen:
   - Initialisieren, Überwachen und Kontrollieren der Leitlinien zur Informationssicherheit
   - Führen des Inventars über die Schutzobjekte
   - Erstellen, Überarbeiten und Überprüfen der Sicherheitsvorgaben (Leitlinien zur Informationssicherheit, Informationssicherheitskonzept, Weisungen, Merkblätter usw.)
   - Kontrollieren des Fortschritts der Umsetzung von Informationssicherheitsmassnahmen
   - Berichten an die Schulpflege über den Stand der Informationssicherheit
   - Berichten an die Schulpflege über zu treffende Informationssicherheitsmassnahmen und Herbeiführen einer Entscheidung
   - Beraten der Mitarbeitenden und die Schulpflege in Fragen der Informationssicherheit
   - Planen, Koordinieren und Umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit
   - Bestimmen der Daten- und Anwendungsverantwortlichen

Art. 27 Anwendungs- und Datenverantwortliche/r

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

2. Aufgaben der Anwendungs- und Datenverantwortlichen
   - Sicherstellen, dass der Zugriff auf Informationssysteme zur Nutzung, Administration, Wartung und zu anderen Zwecken nur durch Berechtigte erfolgt
   - Bestimmen, wer auf die Anwendung in welcher Form Zugriff hat
   - Klassifizieren der Daten, die in ihrem Verantwortungsbereich bearbeitet werden (Vertraulichkeit, Integrität, Verfügbarkeit)
   - Verantwortung für den sicheren Betrieb ihrer Anwendung (Vertraulichkeit und Integrität der Datensammlungen, Verfügbarkeit der Anwendung und Datensammlungen)
   - Regeln der Massnahmen für die Informationssicherheit sowie deren Kontrolle und Verantwortung für die Dokumentation der Sicherheitsvorkehrungen
   - Kontrollieren der Erfüllung der Datenschutz- und Informationssicherheitsbestimmungen
   - Erstellen von Notfallplänen für längere Ausfälle

- Informationsstelle für die in ihrem Verantwortungsbereich liegenden Anwendungen und Datensammlungen
- Verantwortung für die Bearbeitung (inklusive Bekannt- und Weitergabe), Archivierung oder Vernichtung der in ihrem Verantwortungsbereich liegenden Daten

Art. 28 Datenschutzberater/in

1. Der Datenschutz und die Informationssicherheit sind für alle Bereiche, in denen personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Die Schulpflege trägt die Gesamtverantwortung für den Datenschutz in der Schule Zumikon. Sie weist die Rolle / Funktion Datenschutzberater/in einer verantwortlichen Person zu. Sie / er arbeitet in dieser Rolle eng mit den Informationssicherheitsverantwortlichen zusammen und ist interne Ansprechperson bei Datenschutzfragen.

2. Aufgaben der Datenschutzberaterin / des Datenschutzberaters:
   - Ansprechperson für die Mitarbeitenden und die Schulpflege in Belangen des Datenschutzes
   - Bindeglied zum Datenschutzbeauftragten bei Fragen zum Datenschutz
   - Ansprechperson für Betroffene (Auskunfts- und Löschbegehren)
   - Berichten an die Schulpflege über den Stand des Datenschutzes
   - Planen, Koordinieren und Umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit

Art. 29 Kontinuierliche Verbesserung der Informationssicherheit

1. Die Schulpflege Zumikon unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Sie gibt mit der periodischen Überarbeitung dieser Leitlinien zur Informationssicherheit die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung. Die Leitlinien werden alle drei Jahre überprüft.

2. Das Informationssicherheitskonzept wird regelmässig alle drei Jahre sowie zusätzlich bei Projekten mit grossen Auswirkungen auf den Datenschutz und die Informationssicherheit auf seine 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.

Art. 30 Anhang A

Der Anhang A ist ein integrierter Bestandteil dieses Reglements.

Art. 31 Inkrafttreten

Das Reglement «Leitlinien zur Informationssicherheit an der Schule Zumikon» tritt am 1. Juni 2024 in Kraft.

Namens der Schulpflege

Dr. Laetitia Dahl Bünger	**Cinzia Bonati**
Schulpräsidentin	Aktuarin