PRIMARSCHULE TRUTTIKON

Allgemeine Richtlinie für Informationssicherheit und Datenschutz

Inhalt

1 Einleitung

Die PS Truttikon 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 allgemeine Richtlinie. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der PS Truttikon angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet die Richtlinie eine Beschreibung der Informationssicherheitsorganisation.

2 Allgemeine Bestimmungen

2.1 Gegenstand und Zweck

Diese Richtlinie regelt die Ziele, die Organisation der PS Truttikon und die allgemeinen Vorgaben in Bezug auf Datenschutz und Informationssicherheit sowie die Prozesse zu deren kontinuierlichen Verbesserung.

2.2 Geltungsbereich

Die Allgemeine Richtlinie für Informationssicherheit und Datenschutz und die damit zusammenhängenden Dokumente (insbesondere die Weisung zur Informationssicherheit, das Rollen- und Berechtigungskonzept, die Massnahmen zur Sensibilisierung der Mitarbeitenden sowie das Notfallkonzept) gelten für alle Mitarbeiterinnen und Mitarbeiter der PS Truttikon.

Vertragspartner, die Daten bearbeiten, werden ebenfalls zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet. Zudem bildet die Technische Richtlinie für den Betrieb von Informationssystemen einen integrierenden Bestandteil für die detaillierte technische Umsetzung der in dieser Richtlinie formulierten Anforderungen.

2.3 Grundlagen

Die gesetzlichen Grundlagen für die PS Truttikon sind:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8)

3 Informationssicherheitsniveau

Die Massnahmen der PS Truttikon zur Sicherstellung von Datenschutz und Informationssicherheit sind auf einen normalen Schutzbedarf auszurichten. Diese Einstufung erfolgt aufgrund

- der Tatsache, dass die PS Truttikon Daten bearbeitet, die einen erhöhten Schutz vor unberechtigten Zugriffen und vor unerlaubten Änderungen benötigen (Personendaten und besondere Personendaten bzw. Persönlichkeitsprofile),
- der Anzahl Schülerinnen und Schüler: 35
- der Unterstützung aller wesentlichen Funktionen und Aufgaben durch IKT- und Netzwerksysteme,
- der Tatsache, dass ein Ausfall von IKT- und Netzwerksystemen die Aufgabenerfüllung nicht beeinträchtigen darf.

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 Mitarbeiterinnen und Mitarbeiter der Schule sind sich ihrer Verantwortung beim Umgang mit Informationen, IKT-Systemen und Anwendungen bewusst. Sie unterstützen die Informationssicherheitsziele.
Verfügbarkeit	Informationen müssen bei Bedarf vorhanden sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Verwaltungsbetrieb haben.
Vertraulichkeit	Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.
Zurechenbarkeit	Informationsbearbeitungen müssen einer Person zugerechnet werden können.

5 Informationssicherheitsorganisation

5.1 Einleitung

Die relevanten Funktionen der Organisation sind festgelegt und in einem Organigramm dokumentiert.

Die Schulpflege, die oder der Datenschutzbeauftragte (DSB) und die für die einzelnen Bereiche zuständigen Daten- und Anwendungsverantwortlichen haben die zentralen Rollen in der Informationssicherheitsorganisation inne.

Die Informationssicherheitsorganisation ermöglicht es, das angestrebte Informationssicherheitsniveau zu erreichen und dieses aufrechtzuerhalten.

5.2 Schulpflege

Die Schulpflege trägt die Gesamtverantwortung für die Informationssicherheit in der PS Truttikon. Sie legt die Leitlinie zur Informationssicherheit fest und genehmigt die für die Informationssicherheit erforderlichen Massnahmen und Mittel. Sie weist die Rolle des Datenschutzbeauftragten (DSB) einer verantwortlichen Person zu.

5.3 Informationssicherheitsverantwortliche/Informationssicherheitsverantwortlicher

Für die Umsetzung der Informationssicherheitsziele, der Überwachung der Einhaltung des angestrebten Sicherheitsniveaus und für die Informationssicherheit ist der DSB verantwortlich.

Die DSB entscheidet über sicherheitsrelevante Fragen und verwaltet allfällige Ausnahmen. Sie/er ist die Anlaufstelle für Hinweise auf Schwachstellen.

Aufgaben der/des DSB:

- Betreuung der IKT-Umgebung der PS Truttikon und Schnittstelle zu externen Betreibern
- Initialisieren, überwachen und kontrollieren der Richtlinien zur Informationssicherheit
- Verwaltung von Domainnamen der PS Truttikon, insbesondere rechtzeitige Verlängerung der Registrierung
- Verwaltung der digitalen Zertifikate (wo vorhanden) inklusive Überwachung der Gültigkeitsdauer

- Anpassen und überprüfen der Sicherheitsvorgaben (Allgemeine Richtlinie für Informationssicherheit und Datenschutz, Technische Richtlinie für den Betrieb von Informationssystemen, Weisung Informationssicherheit und Datenschutz, Rollen- und Berechtigungskonzept, Betriebsdokumentation usw.)
- Kontrollieren des Fortschritts der Umsetzung von Informationssicherheitsmassnahmen
- Berichten an die Schulpflege über zu treffende Informationssicherheitsmassnahmen und Herbeiführung von Entscheiden
- Erteilung von verbindlichen Anordnungen zur Abwehr von unmittelbar drohenden Gefahren bei Informationssicherheitsvorfällen
- Austausch mit internen und externen Stellen über Informationssicherheitsvorfälle im Bereich Informationssicherheit unter Wahrung der Informationsklassifizierung und Vertraulichkeit, wo nötig
- Beraten der Mitarbeiterinnen und Mitarbeiter sowie der Schulpflege in Fragen der Informationssicherheit
- Umsetzung und Pflege des übergreifenden Rollen- und Berechtigungskonzepts
- Ansprechperson für die Mitarbeiterinnen und Mitarbeiter sowie für die Schulpflege in Belangen des Datenschutzes
- Bindeglied zur kantonalen Datenschutzbeauftragten (DSB) bei Fragen zum Datenschutz
- Zuständige Person für die Einhaltung der gesetzlichen Meldepflicht bei Datenschutzvorfällen
- 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 Datenschutz

6 Regelung von Ausnahmen

Der DSB entscheidet über Ausnahmen von den Richtlinien und Weisungen. Für jede Ausnahme ist ein Zeitpunkt, eine Dauer, die antragsstellende sowie verantwortliche Person zu definieren. Die bestehenden Ausnahmen sind periodisch zu überprüfen.

7 Kontinuierliche Verbesserung der Informationssicherheit

Die Schulpflege unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Sie geben mit der periodischen Überarbeitung dieser Richtlinie zur Informationssicherheit und den dazugehörigen Richtlinien und Weisungen die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung vor.

8 Informationssicherheitsmassnahmen

Aus der Definition der Informationssicherheitsziele ergeben sich folgende Massnahmen. Sie sind angelehnt an die Besonderen Informationssicherheitsrichtlinien des Kantons Zürich.

8.1 Mobiles Arbeiten und mobile Geräte

Falls der Einsatz von mobilen Geräten inklusive der allfälligen Verwendung von privaten Geräten (Bring Your Own Device) für dienstliche Zwecke durch die Mitarbeiterinnen und Mitarbeiter der PS Truttikon zugelassen ist, sind die Voraussetzungen dafür geregelt.

8.2 Personalsicherheit

Mitarbeiterinnen und Mitarbeiter werden auf die Verpflichtungen in Bezug auf den Datenschutz und die Informationssicherheit hingewiesen.

8.3 Schulungsmassnahmen in Informationssicherheit

- Alle Mitarbeiterinnen und Mitarbeiter werden informiert und sensibilisiert.

- Alle Mitarbeiterinnen und Mitarbeiter, die mobile IKT-Systeme nutzen, werden auf die spezifischen Risiken der Informationssicherheit sensibilisiert .
- Schulungen für Informationssicherheit beinhalten folgende Minimalanforderungen:
  - Das Bekenntnis der Mitarbeiterinnen und Mitarbeiter zur Informationssicherheit der PS Truttikon.
  - Die Notwendigkeit, sich mit der Thematik Informationssicherheit auseinanderzusetzen (z.B. Weisung zur Informationssicherheit).
  - Die persönliche Verantwortung für den Schutz von Informationen.
  - Die Abläufe der Informationssicherheit (z.B. Meldung von Informationssicherheitsvorfällen).

8.4 Informationshandhabung

Informationen werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet. Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen. Die Vertraulichkeit ist jederzeit sicherzustellen.

Informationen werden nach Ablauf der vorab definierten Aufbewahrungsdauer dem zuständigen Archiv angeboten. Informationen, die das zuständige Archiv nicht übernimmt, werden sicher vernichtet.

8.5 Verwendung von Wechselmedien

Der Einsatz von Wechselmedien erfolgt kontrolliert, darauf enthaltene dienstliche Daten werden vor Zugriff von Dritten und Verlust geschützt.

8.6 Identitäts- und Zugriffskontrolle

Organisationseigene Werte werden mit geeigneten Massnahmen vor nicht autorisiertem Zugang und Zugriff geschützt. Dieser Schutz umfasst die Authentifizierung (Prüfung, ob die Nutzerin/der Nutzer derjenige ist, für den sie/er sich ausgibt) und Autorisierung (Prüfung, ob die Nutzerin/der Nutzer zugriffsberechtigt ist).

Es gelten die folgenden Grundsätze:

- Der Zugriff auf die Informationen ist durch ein Rollen- und Berechtigungskonzept geregelt
- Berechtigungen werden nach einheitlichen Prozessen vergeben, angepasst und auch wieder gelöscht
- Die Zugriffsberechtigungen für Behördenmitglieder, Mitarbeiterinnen und Mitarbeiter sowie für Lernende auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben geeignet und erforderlich.
- Technische Konten und Benutzerkonten sind einer verantwortlichen Person zugewiesen.
- Bei Austritt von Mitarbeiterinnen und Mitarbeitern werden deren Zugriffsrechte umgehend entfernt bzw. deaktiviert. Verwaltungseigene Hardware wird spätestens bei Austritt zurückgenommen.
- Die Art und Stärke der Authentifizierung werden durch die Klassifizierung der Information und die Exponiertheit der Anwendung bestimmt, auf die der Zugriff erfolgen soll.
- Zugriffsrechte für administrative Zugriffe werden restriktiv und kontrolliert vergeben.
- Es ist jederzeit nachvollziehbar, wer welche Zugriffsrechte besitzt.

8.7 Passwörter

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

8.8 Physische Sicherheit und Schutz vor Umwelteinflüssen

8.9 Sicherheit von Informationssystemen

Neue Informationssysteme werden im Inventar der PS Truttikon nachgeführt, bei Bedarf werden die Auswirkungs- und Bedrohungsanalyse und die Schutzmassnahmen angepasst.

Alle Informationssysteme (Server, Clients und Netzwerkkomponenten) werden regelmässig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.

Die Informationssysteme werden nach der Beschaffung sicher installiert, konfiguriert und betrieben (gemäss anerkannten Sicherheitsstandards), mit einem Änderungsmanagement verwaltet und in einem geregelten Prozess ausser Betrieb genommen.

Informationen zu Verwaltungstätigkeiten werden bei der elektronischen Übertragung und dem physischen Transport in Abhängigkeit ihrer Schutzstufe vor unbefugter Kenntnisnahme und Bearbeitung geschützt.

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

8.10 Datensicherung und -wiederherstellung

Datensicherungen werden regelmässig durchgeführt. Es ist sichergestellt, dass Datensicherungen geographisch abgetrennt von den produktiven Daten aufbewahrt und vor Zugriff geschützt werden.

8.11 Protokollierung

Aktivitäten der Benutzerinnen und Benutzer auf den IKT-Systemen der PS Truttikon können aus Gründen der Nachvollziehbarkeitspflicht wie auch der Funktionsüberwachung, der Sicherheit, der Integrität und der Verfügbarkeit aufgezeichnet werden.

Eine personenbezogene Auswertung ist nur nach vorgängiger Information der Benutzerin respektive des Benutzers möglich.

8.12 Auslagerung von Datenbearbeitungen (Outsourcing)

Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet.
Jeder Outsourcing-Vertrag enthält mindestens Regelungen zu folgenden Themen:

- Gegenstand und Umfang der Datenbearbeitung
- Verantwortung (wer ist wofür verantwortlich)
- Verfügungsmacht (immer beim öffentlichen Organ)
- Zweckbindung (Daten dürfen nur für Vertragszwecke bearbeitet werden)
- Bekanntgabe von Informationen (Voraussetzungen für Bekanntgabe an Dritte)
- Geheimhaltungsverpflichtungen (Hinweis auf Amtsgeheimnis)
- Rechte Betroffener (Umgang mit Auskunftsbegehren)
- Informationssicherheitsmassnahmen (organisatorisch/technisch)
- Kontrollmöglichkeit des öffentlichen Organs oder externer Prüfstellen
- Unterauftragsverhältnisse (Offenlegung, Änderung nur mit Bewilligung)
- Entwicklung und Wartung (Regelung für den Beizug Dritter)
- Orte der Datenbearbeitung (Schweiz, Ausland mit gleichwertigem Datenschutzniveau, ansonsten Schutz durch zusätzliche Massnahmen)
- Cloud Computing (wenn genutzt, den zusätzlichen Risiken angepasste Massnahmen)
- Sanktionen (Konventionalstrafe für schwere Vertragsverletzungen)
- Vertragsdauer und Voraussetzungen der Vertragsauflösung
- Verhältnis zu allgemeinen Vertragsbedingungen (wenn vorhanden, Vorrang des Vertrags)
- Anwendbares Recht (schweizerisches Recht)
- Gerichtsstand (schweizerischer Gerichtsstand im Kanton Zürich)

Benötigt eine externe Stelle oder der interne IKT-Betrieb den Einsatz von Fernwartungszugängen, werden diese nur nach entsprechendem Antrag freigegeben und auf die nötigsten Systeme und Zeiten begrenzt. Vor der Gewährung von Fernwartungszugängen erfolgt eine angemessene Sicherheitsüberprüfung, eine Geheimhaltungsverpflichtung wird unterzeichnet und entsprechende vertragliche Regelungen werden abgeschlossen. Dasselbe gilt für den Einsatz von Fremdpersonal (z.B. temporäre Mitarbeiterinnen oder Mitarbeiter).

8.13 Umgang mit Informationssicherheitsvorfällen

Bei Informationssicherheitsvorfällen erfolgt durch die bzw. den DSB eine Klassifizierung und wenn nötig sofortige Rapportierung an die Schulpflege. Entsprechende interne Prozesse und Verfahren für Meldung,

Mögliche Informationssicherheitsvorfälle sind (nicht abschliessend):
- Verlust, unberechtigte bzw. unbeabsichtigte Löschung oder Vernichtung von Daten, Kopien von Daten oder von Datenträgern
- Veränderung oder Manipulation von Informationen
- Unberechtigter Zugriff oder Bekanntgabe an Unbefugte
- Funktionalität eines oder mehrerer Informationssysteme gestört oder nicht mehr vorhanden

Bei meldepflichtigen Informationssicherheitsvorfällen (Gefährdung von Grundrechten durch die unbefugte Bearbeitung oder den Verlust von Personendaten) erstattet die Schulpflege unverzüglich nach Bekanntwerden des Vorfalls bei der DSB Meldung (§ 12a IDG). Bei Zweifeln über das Vorliegen einer Meldepflicht erfolgt eine unverzügliche Kontaktaufnahme mit der DSB. Im Notfallkonzept sind mögliche Informationssicherheitsvorfälle und Massnahmen zu definieren.

Alle Informationssicherheitsvorfälle werden nachvollziehbar dokumentiert. Die Informationen sind als vertraulich zu betrachten.

8.14 Risikoanalyse / Notfallplanung

Für die PS Truttikon wird eine Auswirkungs- und Bedrohungsanalyse geführt (siehe entsprechende Vorlage). Es werden gemäss der Risikoabschätzung geeignete Massnahmen definiert und umgesetzt.

Die Risikoanalyse dient ebenfalls als Grundlage für das Notfallkonzept der PS Truttikon(siehe entsprechende Vorlage). Das Notfallkonzept beschreibt die Notfallplanung für Geschäftsprozesse und/oder Ressourcen (Schutzobjekte), um die Aufrechterhaltung und Wiederherstellung der ordnungsmässigen Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten.

Die Notfallmassnahmen sind regelmässig und bei veränderten Rahmenbedingungen zu überprüfen und zudem regelmässig zu testen.

Details sind im Notfallkonzept und der Auswirkungs- und Bedrohungsanalyse zu finden.

9 Genehmigung und Inkrafttreten

Ein widerrechtliches oder weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit kann straf-, zivil- und/oder personalrechtliche Konsequenzen haben.

Beschlossen durch die Schulpflege mit Beschluss

Truttikon, Mai 2025 PS Truttikon Schulpflege