Informationssicherheits- und Datenschutzkonzept

1. Einleitung

Die zunehmende Digitalisierung und der verstärkte Austausch von Daten stellen Bildungsinstitutionen vor neue Herausforderungen im Bereich des Datenschutzes und der Informationssicherheit. Die Gewerbliche Berufsschule Wetzikon (GBW) verarbeitet eine Vielzahl personenbezogener Daten von Lernenden, Lehrpersonen und Mitarbeitenden. Dieses Konzept definiert die Grundsätze und Massnahmen zur Sicherstellung des Datenschutzes sowie der Informationssicherheit im Einklang mit dem revidierten Datenschutzgesetz der Schweiz (nDSG) und relevanten kantonalen Bestimmungen.

2. Grundsätze des Datenschutzes gemäss nDSG

Zur Sicherstellung des Datenschutzes gelten folgende Grundsätze:

- **Rechtmässigkeit, Treu und Glauben**: Die Bearbeitung von Personendaten erfolgt in Übereinstimmung mit dem nDSG und kantonalen Vorschriften.
- **Zweckbindung**: Daten werden nur für den festgelegten schulischen oder administrativen Zweck erhoben und verarbeitet.
- **Verhältnismässigkeit**: Die Datenbearbeitung erfolgt nur im notwendigen Umfang.
- **Richtigkeit**: Die Daten müssen aktuell und korrekt sein.
- **Transparenz**: Betroffene Personen werden über die Datenbearbeitung und ihre Rechte informiert.
- **Datensicherheit**: Angemessene technische und organisatorische Massnahmen (TOMs) werden ergriffen, um Daten zu schützen.
- **Schutz besonders schützenswerter Daten**: Gesundheitsdaten, disziplinarische Massnahmen und andere sensible Daten unterliegen besonderen Schutzanforderungen.

3. Informationssicherheitsstrategie der GBW

3.1 Schutz der Vertraulichkeit, Integrität und Verfügbarkeit (CIA-Prinzip)

- **Vertraulichkeit**: Zugriff auf personenbezogene Daten ist auf befugte Personen beschränkt.
- **Integrität**: Daten müssen korrekt und vor unbefugter Manipulation geschützt sein.
- **Verfügbarkeit**: Systeme und Daten sollen im Schulbetrieb jederzeit verfügbar sein.

3.2 Massnahmen zur Informationssicherheit

- **Zugangskontrollen**: Strenge Authentifizierungsverfahren (z. B. Zwei-Faktor-Authentifizierung) und Zugriffsbeschränkungen auf IT-Systeme.
- **Datenverschlüsselung**: Sensible Daten werden verschlüsselt übertragen.
- **Backup- und Wiederherstellungsverfahren**: Regelmässige Backups und Notfallpläne für den Fall von Datenverlust oder Cyberangriffen.
- **Sicherheitsbewusstsein und Schulung**: Schulung aller Mitarbeitenden und Lehrpersonen zu Datenschutz- und Cybersicherheitsrichtlinien.
- **Monitoring und Audits**: Laufende Überwachung und regelmässige Sicherheitsprüfungen von Microsoft (Azure).

4. Verantwortlichkeiten

- **Schulleitung**: Übernimmt die Gesamtverantwortung für Datenschutz und Informationssicherheit an der GBW.
- **Datenschutzverantwortlicher (DSV)**: Koordination und Umsetzung der datenschutzrechtlichen Anforderungen gemäss nDSG.
- **IT-Sicherheitsbeauftragter**: Verantwortlich für die technische Sicherheit der Systeme.
- **Lehrpersonen und Mitarbeitende**: Verantwortlich für den sicheren Umgang mit Daten im Schulalltag.

5. Notfall- und Reaktionsplan bei Datenschutzverletzungen gemäss nDSG

Massnahmen bei Datenschutzverletzungen:

1. **Erfassung des Vorfalls**: Meldung an die Datenschutzverantwortlichen und IT-Support.
2. **Analyse und Massnahmen**: Sofortmassnahmen zur Schadensbegrenzung (z. B. Sperrung betroffener Zugänge, Wiederherstellung von Daten).
3. **Meldung an die Behörden**: Die kantonalen Schulen und das Mittelschul- und Berufsbildungsamt sind verpflichtet, dem Bundesamt für Cybersicherheit (BACS) Cybervorfälle innerhalb von 24 Stunden nach deren Entdeckung zu melden. Bei den Schulen obliegt die Meldepflicht den Rektorinnen und Rektoren. Cybervorfälle können mittels entsprechendem Online-Formular auf der Website des BACS gemeldet werden. Sind bei einem Cybervorfall auch Personendaten betroffen, so muss zusätzlich eine Meldung an die Datenschutzbeauftragte des Kantons Zürich erfolgen: Datenschutzvorfall melden | DSB Kanton Zürich
4. **Kommunikation an Betroffene**: Falls notwendig, Information der betroffenen Personen über das Risiko und empfohlene Schutzmassnahmen.
5. **Nachbearbeitung**: Anpassung der Sicherheitsmassnahmen zur Vermeidung künftiger Vorfälle.

6. Notfallkonzept bei Cyberattacken

Ein Cyberangriff kann gravierende Auswirkungen auf die IT-Infrastruktur und den Schulbetrieb haben. Um angemessen auf solche Bedrohungen zu reagieren, definiert die GBW folgende Notfallstrategie:

6.1 Prävention

- Regelmässige Sicherheitsupdates und Patch-Management für alle IT-Systeme.
- Mitarbeiterschulungen zur Sensibilisierung für Phishing, Social Engineering und andere Cyberbedrohungen.
- Regelmässige Backups wichtiger Daten, die an einem separaten, sicheren Ort gespeichert werden.
- Implementierung von Intrusion Detection Systems (IDS) zur frühzeitigen Erkennung von Angriffen.

6.2 Sofortmassnahmen bei einem Cyberangriff

- Erkennung des Angriffs: Verdächtige Aktivitäten sofort an den IT-Support melden.
- Isolierung betroffener Systeme: Infizierte Geräte vom Netzwerk trennen, um eine weitere Ausbreitung zu verhindern.
- Sicherung von Beweisen: Logs und betroffene Dateien sichern, um die Ursache des Angriffs zu analysieren.

- Aktivierung des Notfallteams: Schulleitung, IT-Abteilung und externe Experten involvieren.
- Kommunikation mit Betroffenen: Falls personenbezogene Daten betroffen sind, werden die notwendigen Meldungen an den Datenschutzbeauftragte des Kantons Zürich und betroffene Personen gemacht.
- Wiederherstellung der Systeme: Daten aus Backups wiederherstellen und Systeme nach Sicherheitsüberprüfung neu aufsetzen.

6.3 Nachbearbeitung und Verbesserung

- Analyse des Angriffs zur Identifikation von Schwachstellen.
- Anpassung der Sicherheitsrichtlinien, um ähnliche Vorfälle künftig zu verhindern.
- Schulung der Mitarbeitenden basierend auf den Erkenntnissen aus dem Angriff.