8303 ASSERSDORF

it-benützungsreglement

8303

Inhaltsverzeichnis

Seite

1.	**Generelles**	**5**
1.1	Vorwort	5
1.2	Revisions-History	5
2.	**Datenschutz**	**5**
2.1	Verantwortung	5
2.2	Sicherheitsrichtlinien des Datenschutzes	5
2.3	Der Faktor Mensch	5
3.	**Betrieb**	**6**
3.1	Beschaffung	6
3.2	Private Hard- und Software	6
3.3	Installation und Konfiguration der Informatikmittel	6
3.4	Berufliche Nutzung der Informatikmittel	6
3.5	Vorgehen zur Nutzung der Informatikmittel	6
3.6	Spezielle Regelung für portable Geräte	6
3.7	Umgang mit Benutzerkennungen und Passwörtern	7
3.8	Internet	7
3.9	E-Mail	7
3.10	Fernzugriff	7
3.11	Unangemessene und private Benutzung	7
3.12	Herunterladen (Download) oder kopieren von Informationen	8
3.13	Kontrollen und Protokollierung	8
3.14	Geräterückgabe	9
3.15	Verhalten bei IT-Störungen und IT-Notfällen	9
3.16	Entsorgung	9
4.	**Risiken, Bedrohungen und Schwachstellen**	**9**
4.1	Malware	9
4.2	Social Engineering	10
4.3	Phishing	10
4.4	Hoax	10
4.5	Fehlende Vertraulichkeit	10
4.6	Anonymität	10

5. Risikominimierung durch Informatikmittel 11
5.1 Antivirenprogramme 11
5.2 Spamschutz 11
5.3 Patchmanagement 11
5.4 Personal Firewall 11

6. Sanktionen 12

7. Inkrafttreten 12

8. Geltungsbereich 12

9. Anhang – Auszug aus dem Strafgesetzbuch 13

Vorbemerkung
Entsprechend dem Grundsatz der Gleichberechtigung von Mann und Frau gelten alle nachstehenden Personen- und Funktionsbezeichnungen, ungeachtet der männlichen Sprachform, für beide Geschlechter.

1. Generelles

Vorwort 1.1

Das IT-Benützungsreglement regelt den Einsatz und den Betrieb der IT-Umgebung in der Gemeinde Bassersdorf. Sämtliche Vorgaben sind verbindlich und müssen von allen Mitarbeitern eingehalten werden.

Die in diesem Dokument aufgeführten Restriktionen dienen dem Datenschutz und der Datensicherheit und wurden vom IT-Verantwortlichen unter Berücksichtigung eines möglichst komfortablen und speditiven Arbeitens ausgearbeitet.

Revisions-History 1.2

Version 1.0	Initial Release
Version 1.1	Kosmetische Anpassungen
Version 2.0	Komplette Überarbeitung unter Berücksichtigung der aktuellen Gegebenheiten

2. Datenschutz

Verantwortung 2.1

Der IT-Verantwortliche ist für die Durchsetzung, die Mitarbeitenden für die Einhaltung dieses Reglements verantwortlich.

Sicherheits-richtlinien des Datenschutzes 2.2

Beim Einsatz der Informatikmittel sind die Sicherheitsrichtlinien des Datenschutzes zu beachten. Die gesamte Übersicht ist abrufbar auf der Webseite des Datenschutzbeauftragten des Kantons Zürich www.datenschutz.ch.

Der Faktor Mensch 2.3

Die IT-Sicherheit ist nicht allein durch technische Massnahmen zu erreichen. Sie bedingt auch ein sachgemässes Verhalten der Mitarbeitenden sowie das Wahrnehmen von gewissen Verantwortungen. Neben dem externen Hacker kann auch der eigene Mitarbeitende dem Unternehmen schaden. Ein fehlerhaftes Verhalten kann grob in die folgenden Kategorien eingeteilt werden:

Beurteilungskriterien	**Beispiele**
Fahrlässigkeit:	Versehentliches Löschen von Informationen
Grobfahrlässigkeit:	Liegenlassen von ungeschützten elektronischen Datenträgern
Vorsatz:	Schädigung der Unternehmung, Bereicherung des Mitarbeitenden, vertrauliche Informationen veräussern oder löschen etc.

3. Betrieb

Beschaffung 3.1

[1]Sämtliche Informatikmittel werden durch den IT-Verantwortlichen beschafft oder deren Beschaffung in Auftrag gegeben. Der Einsatz von privaten Geräten und/oder Software ist generell untersagt und kann nur in Ausnahmefällen und nach Rücksprache mit dem IT-Verantwortlichen bewilligt werden.

[2]Die Gemeinde Bassersdorf beschafft die Informatikmittel nach den kommunalen Submissionsrichtlinien.

Private Hard- und Software 3.2

Aus Sicherheits- und Urheberrechtsgründen ist es den Mitarbeitenden untersagt, ohne Einbezug des IT-Verantwortlichen Software aus dem Internet herunter zu laden oder anderweitig fremde/private Produkte (Software und/oder Hardware wie beispielsweise private Wechseldatenträger) auf seinem Computer zu installieren und zu verwenden. Zudem dürfen Betriebs- und Applikationsprogramme ohne entsprechende Lizenz nicht anderweitig installiert werden.

Installation + Konfiguration der Informatikmittel 3.3

Die Informatikmittel werden durch den IT-Verantwortlichen nach dessen Richtlinien und Standards eingerichtet und gewartet. Die Installation von privater Hard- und/oder Software ist grundsätzlich untersagt. In speziellen Fällen ist die ausdrückliche Zustimmung des IT-Verantwortlichen erforderlich.

Berufliche Nutzung der Informatikmittel 3.4

Alle Informatikgeräte (z.B. PCs, Laptops, PDAs, Smartphones, Mobiltelefone) und Anwendungen sind für geschäftliche Zwecke, d.h. zur Erfüllung der zugewiesenen beruflichen Aufgaben, einzusetzen. Der IT-Verantwortliche kann den Gebrauch von Informatikgeräten ausserhalb des Arbeitsplatzes bewilligen, wenn eine geschäftliche Notwendigkeit vorliegt. Er trägt die Verantwortung für die vollständige und korrekte Instruktion der Mitarbeitenden.

Vorgehen zur Nutzung der Informatikmittel 3.5

Die Mitarbeitenden erhalten mit der erstmaligen Nutzung von Informatikmitteln dieses Reglement und bestätigen dessen inhaltliche Kenntnisnahme und Befolgung mit ihrer Unterschrift. Für jeden Mitarbeitenden wird in der Folge ein persönlicher Login-Name für den Zugang zum Netzwerk sowie für E-Mails und Internet erstellt.

Spezielle Regelung für portable Geräte 3.6

Portable Geräte (u.a. Laptops, PDAs, Smartphones, Mobiltelefone) unterliegen denselben Bestimmungen wie die stationären Geräte. Es darf ohne ausdrückliche Anweisung keine Software installiert werden. Portable Geräte dürfen auf keinen Fall von Drittpersonen verwendet werden. Der designierte Benutzer ist verantwortlich für die Daten auf den portablen Geräten.

Umgang mit Benutzerkennungen und Passwörtern

3.7 Persönliche Benutzerkennungen und dazugehörige Passwörter dürfen niemals für eine Benutzung an Dritte weitergegeben werden. Die Mitarbeitenden sind für den Gebrauch der vorhandenen Zugangskontrolleinrichtungen und -massnahmen (z.B. Passwort, Passwortwahl, -aufbau und -verwahrung usw.) verantwortlich.

Internet

3.8 Alle am Netzwerk der Gemeinde Bassersdorf angeschlossenen Geräte haben ausschliesslich den Internet-Zugang des LEUnet's zu verwenden. Es besteht kein Rechtsanspruch auf den Zugang zum Internet. Der IT-Verantwortliche behält sich das Recht vor, Informationen mit ungeeignetem Inhalt (z.B. pornografisch, rassendiskriminierend, unethisch, unmoralisch) oder mit erkennbaren Risiken für die Verwaltung (Virengefahr) zu sperren oder zu filtern.

E-Mail

3.9 [1]E-Mails sind zur Beschleunigung und Vereinfachung von Vorgängen gegenüber der Briefpost und Fax vorrangig zu nutzen, sofern keine technischen, rechtlichen oder wirtschaftlichen Gründe entgegenstehen.

[2]Die automatische Umleitung von E-Mails ins Internet (z.B. bei Abwesenheit) an E-Mail-Adressen ausserhalb der Verwaltung (z.B. die eigene private Mailbox) ist nicht erlaubt. In berechtigten Fällen wird ein alternativer Zugang eingerichtet.

[3]Besonders schützenswerte, wie personenbezogene Informationen, dürfen nicht unverschlüsselt via E-Mail nach Aussen versendet werden. Dies gilt nicht nur für den Inhalt von E-Mails, sondern auch für beigefügte Dokumente/Anlagen (Attachments).

Fernzugriff

3.10 Ein Fernzugriff auf das Netzwerk der Gemeinde Bassersdorf ist nicht erlaubt. Die dazu technischen Voraussetzungen sind nicht implementiert.

Unangemessene und private Benutzung

3.11 [1]Die Benutzung der Computer, des Internets und von E-Mail muss unter Berücksichtigung der Interessen der Gemeinde Bassersdorf erfolgen, wobei insbesondere rechtliche und operationelle Risiken auszuschliessen sind.

[2]Es ist insbesondere verboten, auf Material mit widerrechtlichem, urheberrechtsverletzendem, rassistischem, beleidigendem, pornografischem oder herabwürdigendem Inhalt zuzugreifen oder solches zu verbreiten. Die private Nutzung der Office-Anwendungen, des Internets und von E-Mail ist erlaubt, sofern die beanspruchten Ressourcen (Arbeitszeit, Netzwerkkapazität, Speicherplatz, Verbindungszeit- und -volumen) vernachlässigbar sind.

[3]Die private Nutzung darf die Erfüllung zugewiesener Aufgaben nicht beeinträchtigen und ist auf das absolut Notwendige zu beschränken. Private Daten (inkl. private E-Mails) sind in einem separaten Ordner abzulegen, der den Namen "Privat" oder "Persönlich" trägt.

[4]Der IT-Verantwortliche behält sich vor, bei unsachgemässem Gebrauch, technische Einschränkungen vorzunehmen oder einzelne Benutzerkennungen zu sperren.

Herunterladen (Download) oder kopieren von Informationen

3.12 [1]Den Mitarbeitenden ist es untersagt, Softwareprogramme aus dem Internet bzw. E-Mail oder von anderen Datenträgern zu kopieren bzw. herunterzuladen und sicherheitsrelevante Ereignisse dann zu installieren oder zu verteilen.

[2]Andere Daten (einschliesslich solcher mit Multimediainhalten) dürfen nur unter den folgenden Bedingungen auf das Netzwerk der Verwaltung heruntergeladen werden:

- Die Daten müssen geschäftsrelevant sein und es dürfen die speziellen Bestimmungen über die private Nutzung nicht verletzt werden;
- Die Daten müssen unter Einhaltung aller Anforderungen des IT-Verantwortlichen sowie den gesetzlichen Bestimmungen beschafft oder verwendet werden.

[3]Die Daten dürfen durch den auf allen Computern der Gemeinde installierten Virenscanner nicht als sicherheitskritisch gemeldet werden.

Kontrollen und Protokollierung

3.13 [1]Die Protokolldaten dienen ausschliesslich der Datensicherung und zur Sicherstellung eines ordnungsgemässen Betriebes, zu Zwecken der Datenschutzkontrolle und der IT-Revision. Sie werden nicht für Zwecke einer präventiven Verhaltens- oder Leistungsbewertung verwendet.

[2]Die Protokollierung berücksichtigt das Datenschutzgesetz des Kantons Zürich, den Schutz der Privatsphäre im Rahmen der anwendbaren gesetzlichen Bestimmungen und weitere Bestimmungen zur Aufbewahrung von Dokumenten.

[3]Um die Sicherheitsanforderungen der Gemeinde Bassersdorf zu gewährleisten, prüft der IT-Verantwortliche und die von ihm bezeichneten Stellen periodisch eine summarische Auswertung (ohne Rückschluss auf bestimmte Personen) der Benutzung der Systeme, Anwendungen, Netzwerke, E-Mail und Internet sowie die auf den Servern abgelegten Datenbestände. Ergibt sich aus der Überprüfung ein Verdacht auf Verstoss gegen dieses Reglement, so bleiben angemessene personenbezogene Prüfungen vorbehalten.

[4]Eine präventive personenbezogene Kontrolle ist nicht erlaubt. Grundsätzlich werden die Mitarbeitenden im Voraus darüber informiert, wenn eine personenbezogene Prüfung vorgenommen wird.

[5]Auf die Vorankündigung kann verzichtet werden, wenn…

- die Datensicherheit, insbesondere die Verfügbarkeit des Systems nicht mehr garantiert werden kann;
- Anhaltspunkte für ein rechtswidriges, insbesondere strafbares Handeln vorliegen.

[6]Wird aufgrund der personenbezogenen Prüfung ein Missbrauch festgestellt, wird die zuständige Dienststelle bzw. die Strafverfolgungsbehörde informiert. Die vorgesetzte Person darf die geschäftlichen Daten überprüfen, soweit dies für seine/ihre Aufsichtstätigkeit notwendig ist. Besondere Geheimhaltungsbestimmungen sowie die Bestimmungen über das Amtsgeheimnis bleiben vorbehalten.

Geräte-rückgabe 3.14

Mitarbeitende sind verpflichtet, bei einem Stellenwechsel oder bei einem Wegfall der Gründe, die zur Geräteabgabe geführt haben, die Geräte zurückzugeben.

Verhalten bei IT-Störungen + IT-Notfällen 3.15

[1]Tritt ein unvorhersehbares Fehlverhalten der Hard- und/oder Software auf, so ist der Mitarbeiter angewiesen, dies umgänglich dem IT-Verantwortlichen zu melden. Der IT-Verantwortliche entscheidet dann über Lösungsweg und Priorität.

[2]Dem Mitarbeiter ist das eigenständige Beheben des Problems strikte untersagt.

Entsorgung 3.16

Der IT-Verantwortliche sorgt dafür, dass ausgediente IT-Komponenten sachgerecht entsorgt werden. Datenträger werden dauerhaft gelöscht oder zerstört.

4. Risiken, Bedrohungen und Schwachstellen

Malware 4.1

Als Malware bezeichnet man Computerprogramme, welche vom Mitarbeitenden unerwünschte (schädliche) Funktionen ausführen. Die Software läuft unbemerkt im Hintergrund. Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien im System zur Folge haben. Zu Malware zählen Viren, Würmer, Trojanische Pferde und Spyware.

Social Engineering 4.2

Der Begriff Social Engineering bezeichnet zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Informationen oder Gegenstände zu gelangen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking.

Phishing 4.3

Phishing (engl. phishing = abfischen) ist eine kriminelle Handlung, die Techniken des Social Engineerings verwendet. Phisher geben sich als vertrauenswürdige Personen aus und versuchen, durch gefälschte elektronische Nachrichten an sensible Daten wie Benutzernamen und Passwörter zu gelangen. Phishing-Nachrichten werden meist per E-Mail oder Instant Messaging versandt und fordern den Empfänger auf, auf einer präparierten Webseite oder am Telefon geheime Zugangsdaten preiszugeben.

Hoax 4.4

Hoax sind Falschmeldungen. Damit keine übereiligen und falschen Handlungen vollzogen werden, ist der IT-Verantwortliche auf jeden Fall zu konsultieren.

Fehlende Vertraulichkeit 4.5

Trotz Einsatz verschiedener Firewall-, Antiviren- und Antispam-Systeme gelangen immer wieder unerwünschte Informationen in das Netzwerk. In den meisten Fällen kommen diese Nachrichten über das Medium E-Mail. Das Bedrohungsausmass variiert stark und kann deswegen nicht genau beziffert werden. Es kann sich um eine simple Werbung handeln, möglich wäre aber auch eine Attacke auf Unternehmensinformationen oder persönliche Angaben. Auch im Internet spielt die Vertraulichkeit eine grosse Rolle. Prinzipiell darf keinem Seiteninhalt vertraut oder keiner Aufforderung zur Bekanntgabe von persönlichen Daten Folge geleistet werden.

Anonymität 4.6

Bei Aktivitäten im Internet fühlen sich viele Benutzer anonym. Diese Anonymität ist jedoch trügerisch. Bei der Kommunikation erfährt die Gegenseite die eigene IP-Adresse, wodurch der Mitarbeitende identifiziert werden kann. Auch Cookies, Browserinformationen oder zuletzt besuchte Seiten können ohne Wissen des Mitarbeitenden weitergegeben werden. Die grösste Gefahr stellt der unbedarfte Umgang mit den eigenen Daten dar. Immer mehr Anwender geben Daten freigiebig für Bonussysteme wie Kundenkarten oder für Preisausschreiben bekannt, ohne zu wissen, was mit diesen geschieht. Trotz zahlreichen Massnahmen wird eine vollumfängliche Anonymität nicht erreicht.

5. Risikominimierung durch Informatikmittel

Die Gemeinde Bassersdorf setzt diverse technische Hilfsmittel zur Minimierung von bestehenden Risiken und Bedrohungen ein. Dazu zählen:

Antiviren-programme 5.1

[1]Zum Schutz vor Viren, wird im Netzwerk der Gemeinde Bassersdorf ein Antivirenschutz eingesetzt, welcher zentral kontrolliert wird. Sämtliche Warnungen und Aktualisierungsvorgänge können so überwacht und nachvollzogen werden. Die verwendeten Schutzmechanismen werden automatisch und permanent mit den neusten Virendefinitionen aktualisiert. Die Daten werden laufend auf unerlaubte Veränderungen überprüft.

[2]Es wäre jedoch trügerisch, sich nur auf diese Technologien zu verlassen. Beim Austausch von Daten über das Internet und beim Einsatz von fremden Datenträgern ist besonders darauf zu achten, dass der Urheber als vertrauenswürdige Person eingestuft werden kann. Bei Virenmeldungen, Unstimmigkeiten oder im Zweifelsfalle muss zwingend der IT-Verantwortliche unverzüglich informiert werden.

[3]Notebooks, PDA's und Smartphones, welche nicht regelmässig über das Netzwerk der Gemeinde Bassersdorf aktualisiert werden können, unterliegen einem erhöhten Risiko. Trotzdem sollte die letzte Aktualisierung der Virendefinitionen nicht länger als drei Tage zurück liegen.

Spamschutz 5.2

Der E-Mail-Provider der Gemeinde Bassersdorf, die ABRAXAS AG, überprüft anhand aktuellster Technologien eingehende E-Mails auf Spam und Viren.

Patchmanagement 5.3

Durch Patches werden in der Regel Sicherheitslecks und/oder Softwarefehler in Betriebssystemen und Softwarelösungen eliminiert. Sämtliche Arbeitsstationen werden täglich auf ihre Aktualität überprüft. Sind neue Patches verfügbar, so werden diese zu einer bestimmten Tageszeit auf den Client heruntergeladen. Ist ein Neustart erforderlich, wird der Benutzer um Erlaubnis gefragt.

Personal Firewall 5.4

Im Intranet wird auf eine personal Firewall verzichtet. Werden mobile Geräte (Notebooks) ausserhalb des Netzwerks der Gemeinde Bassersdorf betrieben, so wird per Richtlinie automatisch die Personal Firewall eingeschaltet.

6. Sanktionen

Eine widerrechtliche, reglementwidrige oder unangemessene Benützung des Internets oder von E-Mail oder jedes andere Verhalten, das einen Verstoss gegen die Pflichten aus dem Arbeitsverhältnis darstellt, können arbeits- und/oder disziplinarrechtliche Sanktionen bis hin zur fristlosen Entlassung sowie strafrechtliche Untersuchung zur Folge haben.

7. Inkrafttreten

[1]Dieses Reglement wurde vom IT-Verantwortlichen der Gemeinde Bassersdorf per sofort in Kraft gesetzt.

[2]Das IT-Benützungsreglement ist von allen Mitarbeitenden, welche Informatikmittel einsetzen, zu unterschreiben. Der IT-Verantwortliche regelt das Vorgehen zur Unterzeichnung.

[3]Änderungen des Reglements haben für die Mitarbeitenden auch ohne schriftliche Bestätigung Gültigkeit, sofern ein anderer Erlass dies nicht erfordert.

8. Geltungsbereich

Dieses Reglement gilt für alle Mitarbeitenden der Gemeinde Bassersdorf.

GEMEINDE BASSERSDORF
IT-Verantwortlicher

9. Anhang – Auszug aus dem Strafgesetzbuch

Art. 135/1 Gewaltdarstellungen

[1]Wer Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände oder Vorführungen, die, ohne schutzwürdigen kulturellen oder wissenschaftlichen Wert zu haben, grausame Gewalttätigkeiten gegen Menschen oder Tiere eindringlich darstellen und dabei die elementare Würde des Menschen in schwerer Weise verletzen, herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

[1bis] Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft,2 wer Gegenstände oder Vorführungen nach Absatz 1, soweit sie Gewalttätigkeiten gegen Menschen oder Tiere darstellen, erwirbt, sich über elektronische Mittel oder sonst wie beschafft oder besitzt.3

[2] Die Gegenstände werden eingezogen.

[3] Handelt der Täter aus Gewinnsucht, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. Mit Freiheitsstrafe ist eine Geldstrafe zu verbinden.

Art. 197 Pornografie

1. Wer pornografische Schriften, Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände solcher Art oder pornografische Vorführungen einer Person unter 16 Jahren anbietet, zeigt, überlässt, zugänglich macht oder durch Radio oder Fernsehen verbreitet, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

2. Wer Gegenstände oder Vorführungen im Sinne von Ziffer 1 öffentlich ausstellt oder zeigt oder sie sonst jemandem unaufgefordert anbietet, wird mit Busse bestraft.

Wer die Besucher von Ausstellungen oder Vorführungen in geschlossenen Räumen im Voraus auf deren pornografischen Charakter hinweist, bleibt straflos.

3. Wer Gegenstände oder Vorführungen im Sinne von Ziffer 1, die sexuelle Handlungen mit Kindern oder mit Tieren, menschlichen Ausscheidungen oder Gewalttätigkeiten zum Inhalt haben, herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Die Gegenstände werden eingezogen.

3bis.1 Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft,2 wer Gegenstände oder Vorführungen im Sinne von Ziffer 1, die sexuelle Handlungen mit Kindern oder Tieren oder sexuelle Handlungen mit Gewalttätigkeiten zum Inhalt haben, erwirbt, sich über elektronische Mittel oder sonst wie beschafft oder besitzt.

Die Gegenstände werden eingezogen.

4. Handelt der Täter aus Gewinnsucht, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. Mit Freiheitsstrafe ist eine Geldstrafe zu verbinden.

5. Gegenstände oder Vorführungen im Sinne der Ziffern 1–3 sind nicht pornografisch, wenn sie einen schutzwürdigen kulturellen oder wissenschaftlichen Wert haben.

Art. 259/1 Öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit

[1] Wer öffentlich zu einem Verbrechen auffordert, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

[2] Wer öffentlich zu einem Vergehen mit Gewalttätigkeit gegen Menschen oder Sachen auffordert, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Art. 261 Störung der Glaubens- und Kultusfreiheit

Wer öffentlich und in gemeiner Weise die Überzeugung anderer in Glaubenssachen, insbesondere den Glauben an Gott, beschimpft oder verspottet oder Gegenstände religiöser Verehrung verunehrt,

wer eine verfassungsmässig gewährleistete Kultushandlung böswillig verhindert, stört oder öffentlich verspottet,

wer einen Ort oder einen Gegenstand, die für einen verfassungsmässig gewährleisteten Kultus oder für eine solche Kultushandlung bestimmt sind, böswillig verunehrt,

wird mit Geldstrafe bis zu 180 Tagessätzen bestraft.

Art. 261/bis 1 Rassendiskriminierung

Wer öffentlich gegen eine Person oder eine Gruppe von Personen wegen ihrer Rasse, Ethnie oder Religion zu Hass oder Diskriminierung aufruft,

wer öffentlich Ideologien verbreitet, die auf die systematische Herabsetzung oder Verleumdung der Angehörigen einer Rasse, Ethnie oder Religion gerichtet sind,

wer mit dem gleichen Ziel Propagandaaktionen organisiert, fördert oder daran teilnimmt,

wer öffentlich durch Wort, Schrift, Bild, Gebärden, Tätlichkeiten oder in anderer Weise eine Person oder eine Gruppe von Personen wegen ihrer Rasse, Ethnie oder Religion in einer gegen die Menschenwürde verstossenden Weise herabsetzt oder diskriminiert oder aus einem dieser Gründe Völkermord oder andere Verbrechen gegen die Menschlichkeit leugnet, gröblich verharmlost oder zu rechtfertigen sucht,

wer eine von ihm angebotene Leistung, die für die Allgemeinheit bestimmt ist, einer Person oder einer Gruppe von Personen wegen ihrer Rasse, Ethnie oder Religion verweigert,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

gemeinde bassersdorf
karl hügin-platz | 8303 bassersdorf | telefon 044 838 85 85
gemeinde@bassersdorf.ch | www.bassersdorf.ch