GEMEINDE LINDAU

Reglement für Informations- und Kommunikationstechnologie (RegIKT)

vom 7. Mai 2013

Inhaltsverzeichnis

1. Allgemeines 4

2. Geltungsbereich 4

3. Informations- und Kommunikationstechnologie 4

4. Risiko 4

5. Warum ein Reglement? 5

6. Mitarbeitende 5

7. Internetzugang 5

8. Rechtsordnung 5

9. Zugangs- und Zugriffschutz 6

10. Passwörter 7

11. Datensicherung, Datenlöschung und Entsorgung von Informationsträgern 7

12. Virenschutz 7

13. Hard- und Software 7

14. Private Web-access und -mail 8

15. Nutzung E-Mail 8

16. Abwesenheit am Arbeitsplatz 8

17. Übertragung von Personendaten, vertraulichen Infos, Programmen 8

18. Privatanwendungen 8

19. Separates, nicht dem Netzwerk angeschlossenes WLAN der Gemeinde 9

20. Downloads 9

21. Kostenpflichtige Infodienste 9

22. Einsatz mobiler Geräte 9

23. Meldepflicht von ausserordentlichen Ereignissen 10

24. Hinweise auf Kontrollen und Protokollierung 10

25. Missbrauch 10

26. Sanktionen bei Wiederhandlung gegen dieses Reglement 10

27. Schlussbestimmungen 11

28. Inkrafttreten 11

Vorbemerkung
Entsprechend dem Grundsatz der Gleichstellung von Frau und Mann gelten alle Personen- und Funktionsbezeichnungen ungeachtet der verwendeten Sprachform für beide Geschlechter.

1. Allgemeines

Dieses Reglement gibt die Nutzung der Informations- und Kommunikationstechnologie vor, im Speziellen den Gebrauch von E-Mail und Internet und die Verwendung mobiler Geräte. Gegenstand des Reglements ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere Personendaten).

Es bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

2. Geltungsbereich

Das Reglement gilt für alle Mitarbeitende der Gemeinde.

Als Mitarbeitende im Sinne dieses Reglements gelten alle fest oder temporär angestellten Mitarbeitenden der Gemeinde sowie die Behörden- und Kommissionsmitglieder.

3. Informations- und Kommunikationstechnologie

Die Informations- und Kommunikationstechnologie-Mittel (der Begriff umschliesst Internet, Email und mobile Geräte) sind sowohl für Unternehmen als auch Privatpersonen wichtige Instrumente für die Beschaffung und den Austausch von Informationen sowie für das Angebot und die Nutzung kommerzieller Dienstleistungen. Dabei sind die Rahmenbedingungen des Datenschutzes und der Informationssicherheit sowohl aus rechtlichen als auch sicherheitsrelevanten Gründen zwingend zu beachten.

Die Datenübermittlung erfolgt über äusserst komplexe Informationsverbindungen, die vom Anwender weder voraussehbar noch vorherbestimmbar sind. Datenverbindungen werden je nach der aktuellen Datenmenge automatisch auf verschiedenste Übertragungssysteme umgeleitet. Der Datenfluss ist in der Folge für den Anwender nicht kontrollierbar. Dennoch können die versandten Informationen von Dritten gelesen und manipuliert werden, sofern zu ihrem Schutz nicht besondere Massnahmen (z.B. Mailverschlüsselungsprogramme) ergriffen wurden. Der normale Mailverkehr – auch in der Gemeinde Lindau – ist nicht verschlüsselt und daher gegenüber unbekannten Dritten grundsätzlich als einsehbar zu betrachten.

4. Risiko

Der Gebrauch des Internets (auch über mobile Geräte) und insbesondere die Verwendung von E-Mail-Systemen bergen in technischer, anwendungsmässiger sowie datenschutzrechtlicher Hinsicht teilweise erhebliche Risiken. Sie sind vom Laien schwer abschätzbar. Eine Schadensbehebung aufgrund der Missachtung von Sicherheitsvorschriften ist nicht nur zeitaufwändig sondern in der Regel auch sehr kostenintensiv. Es gilt daher, diese Risiken durch die Einhaltung bestimmter Anwendungsvorschriften weit möglichst auszuschalten.

5. Warum ein Reglement?

Das vorliegende Benützungsreglement von Informations- und Kommunikationstechnologie, nachstehend ‚Reglement' genannt, zeigt den sicheren Umgang mit elektronischen Werkzeugen auf und markiert den Wirkungsrahmen, innerhalb dessen sich die Mitarbeiter der Gemeinde Lindau gefahrlos bewegen können. Widerhandlungen gegen das Reglement begründen arbeits- und / oder strafrechtliche Konsequenzen. Die Erstellung eines solchen Reglements wird auch vom Datenschutzbeauftragten zwingend verlangt.

6. Mitarbeitende

Die Mitarbeitenden sind verpflichtet, die gesetzlichen Vorgaben und das Reglement zu beachten. Sie haben die Kenntnisnahme dieses Reglements unterschriftlich zu bestätigen.

Die Mitarbeitenden sind verpflichtet, die ihnen zur Verfügung gestellten IKT-Mittel recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere mit Personendaten und besonderen Personendaten, sorgfältig umzugehen.

Die Mitarbeitenden melden alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden an und Verlust von Hardware und Software dem IT-Verantwortlichen und der IT-Abteilung der Stadt Illnau-Effretikon (welche unsere IT betreibt). Diese Stellen sind verpflichtet, bei gravierenden Vorfällen den Gemeindeschreiber zu informieren.

7. Internetzugang

Alle Mitarbeiter der Gemeinde Lindau mit einem IT-Arbeitsplatz wird im Normalfall ein Internet-Zugang am PC des Arbeitsplatzes ermöglicht. Ein Rechtsanspruch für diesen Anschluss besteht nicht.

Das Internet ist grundsätzlich für geschäftliche Zwecke, d.h. zur Erfüllung der zugewiesenen beruflichen Aufgaben, einzusetzen.

Der Internetanschluss kann bei Widerhandlungen gegen das Reglement jederzeit und ohne Vorankündigung gesperrt werden. Ausdrücklich vorbehalten bleibt das Recht, Webseiten mit ungeeignetem Inhalt (beispielsweise pornografisch, rassendiskriminierend, unethisch, unmoralisch) oder mit erkennbaren Risiken (Virengefahr) zu sperren. Das Vorgehen im Ereignisfall erfolgt analog der Bestimmungen, wie sie im Punkt „Missbrauch" umschrieben sind.

8. Rechtsordnung

Unabhängig von den Bestimmungen in diesem Reglement gelten ohne Weiteres u.a. folgende übergeordnete Vorschriften:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41
- Gemeindegesetz (GG, LS 131.1)
- Informatiksicherheitsverordnung (LS 170.8)
- Schweizerisches Strafgesetzbuch (StGB)
- Gemäss den Bestimmungen des Schweizerischen Strafgesetzbuches (StGB) sind das Abrufen und Publizieren folgender Inhalte auf Internet strafbar:
- Gewaltdarstellungen, Art. 135 StGB;
- Pornographie, Art. 197 Ziff. 1 + 3 StGB;

- Öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit, Art. 259 StGB;
- Strafbare Vorbereitungshandlungen, Art. 260bis 151 StGB;
- Kriminelle Organisation, Art. 260ter 153 StGB;
- Gefährdung der öffentlichen Sicherheit mit Waffen, Art. 260quater 154 StGB;
- Störung der Glaubens- und Kultusfreiheit, Art. 261 StGB;
- Rassendiskriminierung im Sinne von Art. 261bis 155 StGB;
- Anleitung oder Anstiftung zu strafbarem Verhalten oder dessen anderweitiger Förderung;
- Unerlaubte Glücksspiele.

Sofern Sie auf strafbare Handlungen im Internet aufmerksam werden, haben Sie grundsätzlich eine Anzeigepflicht (vgl. § 21 der kantonalen Strafprozessordnung StPO). Falls Sie auf solche Inhalte stossen, melden Sie diese umgehend dem IT-Verantwortlichen oder der IT-Abteilung der Stadt Illnau-Effretikon.

9. Zugangs- und Zugriffschutz

Die Mitarbeitenden haben zu verhindern, dass Unbefugte Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen (z.B. Servicetechniker usw.) oder internes Personal (z.B. Reinigungspersonal, Behördenmitglieder) in den Büroräumlichkeiten auf, ist dafür zu sorgen, dass diese keinen unbefugten Zugang zu Informationen erhalten.

Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Abschliessen des Büros, Sperren oder Herunterfahren des PC).

Ausdrucke oder Kopien mit vertraulichen Informationen sind umgehend aus allgemeinen Geräten zu entfernen.

Die Mitarbeitenden dürfen nur ihre persönlichen Benutzerkonten verwenden. Sie sind für die auf ihre Kontis erfolgten Zugriffe verantwortlich.

Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten.

Der Verlust von Schlüsseln, Badges, usw. ist umgehend zu melden. Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist der Personaldienst umgehend zu informieren.

Allen Mitarbeitern ist jegliches Abspeichern von geschäftlichen Daten auf privaten Geräten verboten.

Behördenmitglieder dürfen geschäftliche Daten nur dann auf privaten Geräten speichern, wenn eine dem Sicherheitsstandard der Gemeinde Lindau entsprechende Zugangssicherung besteht. Es ist insbesondere verboten, Daten auf Geräten zu speichern, die auch anderen Familienmitgliedern oder Mitarbeitenden zugänglich sind.

Austretende Behördenmitglieder haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und die ausserhalb der Stadtverwaltung bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht) oder der Verwaltung zurückgegeben wurden.

10. Passwörter

Passwörter sind vertraulich zu behandeln. Es ist verboten, eigene Benutzererkennungen und dazugehörige Passwörter unberechtigten Dritten zur Kenntnis zu bringen. Passwörter sind regelmässig - mindestens einmal jährlich - zu ändern.

Passwörter müssen mindestens acht Stellen lang sein und sollen eine Kombination von Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten.

Passwörter die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt. Geschäftlich genutzte Passwörter dürfen nicht privat verwendet werden.

11. Datensicherung, Datenlöschung und Entsorgung von Informationsträgern

Geschäftsbezogene bzw. geschäftsrelevante Daten müssen auf Serverlaufwerken gespeichert bzw. archiviert werden.

Nicht mehr benötigte Daten müssen von Datenträgern (z.B. USB-Datenträger, Speicherkarten usw.) unwiederbringlich gelöscht werden (einfaches Löschen genügt nicht).

Nicht mehr benötigte Informationsträger (z.B. CD-ROM, USB-Datenträger usw.), die vertrauliche Informationen enthalten oder einmal enthielten, sind physikalisch zu vernichten (z.B. Shreddern).

12. Virenschutz

Die Mitarbeitenden dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder umkonfigurieren.

E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind im Hinblick darauf, dass sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten, vorsichtig zu behandeln. Deren Beilagen dürfen keinesfalls geöffnet werden. Jeder Verdacht auf Virenbefall muss sofort dem IT-Verantwortlichen oder der IT-Abteilung der Stadt Illnau-Effretikon gemeldet werden.

13. Hard- und Software

Die Mitarbeitenden dürfen keine Software und keine privaten Hardware-Erweiterungen, insbesondere keine Kommunikationseinrichtungen und externe Massenspeicher installieren bzw. anschliessen. Geschäftlich genutzt Speichermedien (z.B. Sticks) dürfen nur für geschäftliche Zwecke verwendet werden.

Die Mitarbeitenden dürfen Informatiksysteme, die am Netzwerk angeschlossen sind, nicht gleichzeitig mit einem Netz oder System ausserhalb des Gemeinde-Netzwerkes verbinden.

Nur der Informatikdienst darf Geräte in die Reparatur oder zur Entsorgung geben. Dieser stellt sicher, dass keine schützenswerten Daten auf diesem Weg die Amtsstelle verlassen.

Änderungen an der Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur vom Administrator vorgenommen werden.

14. Private Web-access und -mail

Externe Internet-Dienste (wie z.B. Online-Dateiablagen, Online-Kalender usw.) oder E-Mail-Systeme dürfen nicht verwendet werden.

15. Nutzung E-Mail

Die Nutzung von E-Mail ist gegenüber der Verwendung von Faxgeräten und Briefpapier zu bevorzugen.

Dabei ist die Mailbox (elektronischer Briefkasten) möglichst oft, mindestens jedoch einmal pro Halbtag auf den Eingang von E-Mails zu kontrollieren. E-Mails sind entweder innert Tagesfrist zu beantworten oder, falls dies nicht möglich ist, ist innert gleicher Frist eine Eingangsbestätigung mit Nennung einer Frist für die Bearbeitung an den Absender zuzustellen.

16. Abwesenheit am Arbeitsplatz

Bei Abwesenheit am Arbeitsplatz von mehr als einem Tag ist der Abwesenheitsassistent zu aktivieren. Dabei ist die automatische Umleitung von E-Mails via Internet an nicht interne E-Mail-Adressen (z. B. die eigene private Mailbox) aus Gründen der Datensicherheit und des Datenschutzes grundsätzlich nicht statthaft. Über Ausnahmen entscheidet der zuständige Abteilungsleiter (bzw. Ressortvorsteher bei Abteilungsleiter) in Absprache mit dem IT-Verantwortlichen.

17. Übertragung von Personendaten, vertraulichen Infos, Programmen

Personendaten und / oder andere vertrauliche Daten dürfen nicht via E-Mail-System im Internet übertragen werden, da der Datenschutz bei der Übertragung nicht gewährleistet werden kann. Dies gilt nicht nur für E-Mail-Meldungen selbst, sondern insbesondere auch für diesen beigefügte Dokumente / Anlagen (so genannte Attachements).

18. Privatanwendungen

Die Nutzung des Internets sowie des E-Mail-Systems für private Zwecke ist zulässig, sofern dabei die Erfüllung zugewiesener Aufgaben nicht beeinträchtigt wird. Dabei sind diese Privatanwendungen während der Arbeitszeit als Ausnahmefälle zu betrachten und auf das absolute Minimum zu beschränken.

Private E-Mails müssen entweder gelöscht oder in einem persönlichen Ordner mit der Bezeichnung „PRIVAT" abgelegt werden.

Ausdrücklich verboten sind:

- die elektronische Übermittlung von Programmen oder Programmteilen inkl. Video und / oder Sounddateien
- die Ausführung von privaten Finanztransaktionen (Telebanking, Börsengeschäfte oder ähnliches
- der Zugriff auf Informationen mit widerrechtlichem, urheberrechtsverletzendem, rassistischem, beleidigendem, pornografischem oder herabwürdigendem Inhalt u. dergleichen oder die Verbreitung / Weiterleitung solcher Inhalte
- die Benutzung von Chat-Diensten

- das Abrufen von E-Mails aus privaten Mailboxen

Über individuelle Ausnahmen entscheidet der zuständige Abteilungsleiter (bzw. Ressortvorsteher bei Abteilungsleiter) in Absprache mit dem Personaldienst.

19. Separates, nicht dem Netzwerk angeschlossenes WLAN der Gemeinde

Die Nutzung des separaten WLAN ist mit privaten Geräten (nicht aber zulässig ist der Zugang in dieses Netz mit gemeindeeigenen Geräten), wobei diese während der Arbeitszeit ebenfalls auf ein absolutes Minimum zu beschränken ist. Verboten ist über dieses Netz ebenfalls der Zugriff auf sämtliche widerrechtlichen Inhalte (vgl. Punkt 18). Es wird darauf hingewiesen, dass dieses Netz datenschutzmässig nur via ein Passwort geschützt ist und namentlich kein Firewall vorhanden ist. Die Nutzung erfolgt auf eigenes Risiko, die Gemeinde lehnt jede Haftung ab.

20. Downloads

Downloads (Herunterladen) von Daten bzw. Dateien (einschliesslich solcher mit Multimediainhalten) sind nur zulässig, wenn es sich um geschäftsrelevante Informationen handelt und deren Ursprung bekannt ist. In Zweifelsfällen ist der IT-Verantwortliche zu kontaktieren.

Ausdrücklich verboten ist das Herunterladen und/oder Installieren von Programmen oder Programmteilen (inkl. Video und / oder Sounddateien, z.B. *.exe)

21. Kostenpflichtige Infodienste

Informationsdienste im Internet, deren Benützung kostenpflichtig ist, dürfen nicht abonniert werden. Über beruflich bedingte Ausnahmen entscheidet der Gemeindeschreiber.

22. Einsatz mobiler Geräte

- Auf mobilen Geräten (z.B. Notebooks, USB-Datenträger, Smartphones usw.) müssen Dokumente mit vertraulichem bzw. schützenswertem Inhalt verschlüsselt gespeichert werden
- Mobile Arbeitsgeräte müssen mit einem Boot-Passwort geschützt werden
- Die Benutzerinnen und Benutzer von mobilen Arbeitsstationen sind selbst für die Datensicherung und die datenschutzgerechte Aufbewahrung verantwortlich
- Mobile Geräte dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden
- Die Geräte dürfen nicht Dritten zur Nutzung überlassen werden
- Der Verlust eines mobilen Gerätes ist unverzüglich dem Leiter Informatikdienst zu melden.
- Es dürfen keine zusätzlichen Applikationen installiert werden. Besteht ein begründeter Bedarf, ist die Genehmigung des Vorgesetzten und des Leiter Informatik einzuholen
- Eine Verbindung zu drahtlosen Netzwerken (z.B. WLAN) ist nur zulässig, wenn eine Verschlüsselung eingesetzt wird
- Drahtlose Komponenten (z.B. Bluetooth, WLAN, Infrarot etc.) sind bei Nichtgebrauch zu deaktivieren
- Die Ortungsdienste sind bei Nichtgebrauch zu deaktivieren

23. Meldepflicht von ausserordentlichen Ereignissen

Ein für den Anwender nicht erklärbares Systemverhalten, nicht nachvollziehbarer Verlust von Daten bzw. Datenveränderungen, unaufgeforderte Verfügbarkeit von gesperrten Diensten, Verdacht auf Missbrauch der eigenen Benutzererkennung etc. sind umgehend dem IT-Verantwortlichen oder der IT-Abteilung der Stadt Illnau-Effretikon zu melden.

Eigene Aufklärungs- und / oder Datenrettungsversuche sind dabei zwingend zu unterlassen; es besteht die Gefahr der Zerstörung wichtiger Spuren und Hinweise!

24. Hinweis auf Kontrollen und Protokollierung

Es wird ausdrücklich darauf hingewiesen, dass das Surf-Verhalten der einzelnen Anwender im Internet bis zum Ausgangspunkt (PC-Arbeitsplatz, mobile Geräte) zurückverfolgt werden kann. Zur Gewährleistung des Schutzes der Gemeinde vor operationellen und rechtlichen Risiken (z.B. Einschleusung von so genannten „Viren“, „Würmern“, „Trojanischen Pferden“ / Urheberrechtsverletzungen etc.) erfolgen periodische Überprüfungen des E-Mail- sowie Internetverkehrs der Mitarbeitenden betreffend Datenmengen sowie Surfzeiten.

Durch Mitarbeitende aufgerufene Websites werden automatisiert nach rechtswidrigen Inhalten gescannt. Bei wiederholt positiver Erfassung erfolgt eine automatisierte Meldung an den Leiter Informatikdienst der Stadt Illnau-Effretikon. Dieser entscheidet über die Information des Gemeindeschreibers.

Das EDV-System erstellt automatisiert Zugriffsprotokolle unter Berücksichtigung der Datenschutzgesetzgebung des Kantons Zürich, insbesondere betreffend des Schutzes der Privatsphäre. Die Protokollinformationen dienen dabei ausschliesslich zu Zwecken der Datenschutzüberprüfung, der IT-Revision, Sicherung von Daten sowie der Gewährleistung eines störungsfreien EDV-Betriebes. Es erfolgt keine personenbezogene Auswertung / Überwachung für Verhaltens- und / oder Leistungskontrollen.

25. Missbrauch

Wird ein Missbrauch von Internet auf Grund der automatischen Protokollierung und dem Resultat von Auswertungen festgestellt, erfolgt eine Information des Leiter Informatikdienstes der Stadt Illnau-Effretikon an den Gemeindeschreiber. In einem solchen Fall kann insbesondere - unter Information des betroffenen Mitarbeiters - eine personenbezogene Überwachung angeordnet werden.

26. Sanktionen bei Wiederhandlung gegen dieses Reglement

Verstösse gegen die Bestimmungen dieses Reglements oder generell widerrechtliches Verhalten im Zusammenhang mit der Anwendung der Internettechnologie der Gemeinde Lindau können nach den Bestimmungen des Personalrechtes und des Strafrechtes geahndet werden, so z.B.

- arbeits- und / oder disziplinarrechtliche Sanktionen
- Abmahnungen
- Sperrung Internet
- Schadenersatzforderungen
- fristlose Entlassung

27. Schlussbemerkung

Dieses Reglement ist allen Mitarbeitern im Sinne einer Dienstanweisung zugestellt und die Anerkennung des Inhaltes durch dieselben schriftlich auf einem separaten Formular, welches in den Personalakten aufbewahrt wird, bestätigt worden.

28. Inkrafttreten

Dieses Reglement hat der Gemeinderat mit Beschluss vom 7. Mai 2013 genehmigt und wird per 1. Juni 2013 in Kraft gesetzt.

Änderungen sind mit Beschluss des Gemeinderates jederzeit möglich.

Lindau, 7. Mai 2013

GEMEINDERAT LINDAU
Bernard Hosang, Präsident
Viktor Ledermann, Schreiber