Gemeindeverband Sozialbereiche Bezirk Rheinfelden

IT-Benutzerrichtlinien

IT-User Policy

Gültig per 01.01.2025

IT-Benutzerrichtlinien

GSBR Gemeindeverband Sozialbereiche Bezirk Rheinfelden

INHALTSVERZEICHNIS

I. Zweck der IT-Benutzerrichtlinien

Diese Benutzerrichtlinien bezwecken

- den unbefugten Zugriff auf das GSBR-Netzwerk zu verhindern
- das Netzwerk vor schädlichen Programmen zu schützen
- sicherzustellen, dass die Benutzer des Netzwerkes ihre Nutzungsrechte und ihre Aufgaben sowie ihre Verantwortung kennen
- den Benutzern bekanntzumachen, wohin sie sich mit welchen Problemen wenden können

II. Kennwörter

Kennwörter authentifizieren den Anwender als rechtmässigen Benutzer im Netzwerk vom GSBR. Sie sind die wichtigste Massnahme, einen rechtmässigen Benutzer von einem nicht autorisierten Benutzer zu unterscheiden. Die Kennwörter bilden somit einen wichtigen Schutz vor nicht autorisierten Anwendern und Eindringlingen.

Die Kennwörter sind jedoch nur ein wirksamer Schutz, solange sie nicht unautorisierten Personen zugänglich gemacht werden oder aber relativ einfach vom entsprechenden Benutzer hergeleitet werden können. Jeder Benutzer des Netzwerkes vom GSBR ist deshalb verpflichtet, folgende Richtlinien bezüglich der Kennwörter strikt einzuhalten:

- das persönliche Kennwort muss unter Verschluss gehalten und darf unautorisierten Personen weder bekannt gegeben noch aufgeschrieben werden
- der Benutzer muss dafür sorgen, dass sein persönliches Kennwort nicht von seiner Person hergeleitet werden kann, d.h. er wählt ein Kennwort, welches keinen Bezug auf seine Person hat
- das Kennwort muss mindestens 10 Zeichen lang sein
- 3 der 4 folgenden Kriterien müssen im Passwort enthalten sein:
  - Großbuchstaben (A bis Z)
  - Ziffern (0 bis 9)
  - Sonderzeichen (zum Beispiel: !, &, /, %)
  - Unicodezeichen (€, @, ®)
- Die letzten 10 Passwörter können nicht wiederverwendet werden
- Regelmässig wird der Benutzer wieder aufgefordert, das Passwort zu ändern.

Die definierte Kennwortrichtlinie wird vom System vorgegeben und erzwungen. Ausnahmen werden nicht erteilt.

Um komplexe Passwörter zu erstellen und diese sicher aufzubewahren, empfehlen wir die Verwendung eines Passwortmanagers.

III. Installation und Berechtigungen

Die Benutzer erhalten ein ihrer Tätigkeit entsprechendes IT-Equipment. Ihnen ist es untersagt, eigenmächtig Programme auf den Arbeitsstationen zu installieren, für welche GSBR über keine Softwarelizenz verfügt. Bei Bedarf von zusätzlicher Software ist ein entsprechender Antrag an den jeweiligen Vorgesetzten zu stellen, welcher die notwendigen Abklärungen trifft und die Software zur Beschaffung bzw. Installation freigibt.

Bei Beschädigung oder Zerstörung der Installation auf der Arbeitsstation durch fehlerhafte Manipulationen des Benutzers wird der ursprüngliche Zustand der Installation wiederhergestellt. Durch diesen Eingriff können alle individuellen Einstellungen sowie alle lokal gespeicherten Daten verloren gehen. Die Verantwortung bezüglich lokal gespeicherter Daten trägt der jeweilige Benutzer und ist für deren Sicherung selbst verantwortlich.

IV. Externer Zugriff auf das Netzwerk

GSBR bietet für das auswärtige Arbeiten für das eigene IT-Equipment einen VPN-Zugriff an.

Für den externen Zugriff sind neben einer erweiterten Identifikation (sog. Multifaktor-Authentifizierung resp. MFA oder 2FA) auch zusätzliche Sicherheitsbestimmungen einzuhalten. Bei Zuwiderhandlung kann die Autorisierung für den externen Zugriff wieder entzogen werden.

A. Erweiterte Identifikation

Für die erweiterte Identifikation wird ein zweiter Authentisierungsfaktor abgefragt. Dies erfolgt mittels der aktiven Bestätigung (App auf dem Mobiltelefon), dass ein VPN-Zugriff tatsächlich initialisiert und gewünscht wurde. Die Identifikation erfolgt demnach mittels

- Benutzername und Kennwort
- Zweiter Faktor (Zugriffsbestätigung mittels App auf dem Mobiltelefon)

Der Benutzer hält den Benutzernamen und das Kennwort unter Verschluss sowie verhindert unbefugten Dritten den Zugriff auf das Mobiltelefon bzw. die App. Der Benutzer meldet einen möglichen Verlust des Mobiltelefons, welches die Authentifizierung sicherstellt, umgehend bei der GSBR-Informatik zwecks Sperrung des Zugangs.

B. Zusätzliche Sicherheitsbestimmungen beim externen Zugriff

Neben der erweiterten Identifikation sowie den in dieser Benutzerrichtlinie allgemein festgelegten Sicherheitsbestimmungen gelten für den externen Zugriff noch zusätzliche Sicherheitsbestimmungen.

a) Zugriff über einen GSBR-Computer

Bei Verwendung eines Computers vom GSBR ***gelten*** keine zusätzlichen Sicherheitsbestimmungen.

b) Zugriff über einen „fremden" Computer

Ein Zugriff über einem dem Benutzer fremden Computer (z.B. im Internetcafé) ist nicht gestattet.

Der Computer darf nicht mit einer offenen Verbindung zum GSBR-Netzwerk, auch für kurze Zeit, verlassen werden; eine offene Verbindung muss vor dem Verlassen immer geschlossen werden (sich komplett abmelden).

Der Benutzer ist dafür verantwortlich, dass vor dem Verlassen des fremden Computers, jegliche lokal gespeicherten Daten gelöscht werden, und zwar auch aus dem Papierkorb. Da jederzeit die Möglichkeit besteht, gelöschte Daten wiederherzustellen, sollte insbesondere bei Zugriff über einen fremden Computer auf das Herunterladen von Daten (lokales Speichern) verzichtet werden. Jedenfalls ist der Benutzer für die weitere Verwendung von solchen Daten verantwortlich.

V. Smartphones

Die Benutzung von Smartphones in Verbindung mit dem GSBR-Netzwerk (Abgleich von Daten, im Speziellen Emails, Kontakte, Kalender etc.) wird angeboten. Es gelten die gleichen Sicherheitsbestimmungen wie für das gesamte GSBR-Netzwerk.

Die Verantwortung bezüglich gespeicherter Daten auf dem Smartphone trägt der jeweilige Benutzer und ist für deren Sicherung selbst verantwortlich.

VI. IT-Support für Benutzer

Dem IT-Support ist grundsätzlich jederzeit Zugang zu den Arbeitsstationen zu gewähren. Üblicherweise wird mit dem Benutzer ein Termin vereinbart. Es kann jedoch vorkommen, dass der IT-Support unangemeldet Zugang zu den Arbeitsstationen haben muss. In diesem Fall ist der Benutzer dazu verpflichtet, ihm den Zugang sofort zu gewähren.

Der IT-Support muss bei Abwesenheiten des Benutzers Zugang zu den Arbeitsstationen haben (Ausnahme: Laptops, welche ausser Haus sind). Der Benutzer ist bei längerer Abwesenheit vom Arbeitsplatz dazu verpflichtet, die Daten zu sichern. Der IT-Support ist im Notfall dazu berechtigt, alle Programme, ohne zu Speichern zu schliessen und die notwendigen Arbeiten am Gerät vorzunehmen.

Der Benutzer ist ebenfalls dazu verpflichtet, bevor er nach Hause geht, den PC ordentlich herunterzufahren.

Beim Verlassen des Arbeitsplatzes ist der Computer zu sperren (Ctrl / Alt / Delete oder Windows-Taste/L).

VII. Sorgfaltspflicht

Der Benutzer verpflichtet sich, dass ihm zur Verfügung gestellte IT-Equipment sorgfältig zu behandeln. Er ist auch dafür besorgt, die IT-Komponenten vor Diebstahl und Beschädigung zu schützen. Bei Diebstahl oder Verlust eines Laptops ist unverzüglich die GSBR-Informatik resp. der IT-Verantwortliche zu benachrichtigen (Geschäftsleitung).

Der Benutzer darf keine technischen Manipulationen an den Geräten vornehmen oder durch Dritte zulassen, welche den Garantiebestimmungen der Hersteller widersprechen. Auch andere technische Manipulationen, wie das Öffnen des Gerätegehäuses sind untersagt.

Bei Störungen sind alle Benutzer verpflichtet, unverzüglich jemanden vom IT-Support zu informieren.

VIII. Datensicherheit

Jeder Benutzer ist grundsätzlich selbst für seine Daten verantwortlich.

Alle Daten, welche sich auf der IT-Infrastruktur vom GSBR befinden, werden täglich gesichert. Lokal gespeicherte Daten sind von diesem Backup ausgeschlossen. Es wird dringend empfohlen, keine Daten Lokal zu speichern. Bei Verlust einer Datei, welche sich auf dem Server befunden hat, kann über den IT-Support die Wiederherstellung der verlorenen Datei beantragt werden.

Datenverluste, welche durch Nichtbeachtung der Ankündigung von Wartungsarbeiten entstehen, liegen in der Verantwortung des betroffenen Benutzers.

IX. Wartungsarbeiten

Um das System vor Ausfällen zu bewahren, sind regelmässige Wartungsarbeiten unumgänglich. Dazu muss sehr oft ein Teil des Systems kurz vom Netz getrennt werden (z.B. für einen Neustart eines Servers).

Ausserordentliche Wartungsarbeiten, welche zu längeren Netzunterbrüchen führen, werden nach Möglichkeit frühzeitig angekündigt und auf Randstunden nach den ordentlichen Servicezeiten verlegt.

Notfallmässige Wartungsarbeiten mit Netzausfall werden mit einer Ankündigungszeit von i.d.R. mindestens 30 Minuten mitgeteilt.

Die Benutzer müssen die entsprechenden Vorkehrungen treffen, damit kein Datenverlust entsteht und sie eventuell weiterarbeiten können (vom Netz getrennt).

X. Software-Lizenzen

Im Netzwerk vom GSBR darf ausschliesslich beim jeweiligen Hersteller lizenzierte Software eingesetzt werden. Der Benutzer darf unter keinen Umständen nicht für GSBFR lizenzierte Software installieren/verwenden.

Weiter gelten die Lizenzbestimmungen der Software-Hersteller.

Bei Zuwiderhandlung gegen die Software-Lizenzbestimmungen ist der fehlbare Benutzer persönlich und vollumfänglich für sein Handeln haftbar.

XI. Computer-Viren

Im Netzwerk vom GSBR ist eine Anti-Virus-Software installiert, welche automatisch erneuert wird und somit die meisten Computer-Viren erkennt. Diese Software kann jedoch nicht garantieren, das Netzwerk von vom GSBR vor allen Computer-Viren zu schützen.

Aus diesem Grund sind alle Benutzer des GSBR-Netzwerkes aufgefordert, folgende Verhaltensregeln strikt einzuhalten.

- E-Mails aus unbekannter Quelle dürfen unter keinen Umständen geöffnet werden; sie müssen sofort gelöscht werden.
- E-Mail-Beilagen aus unbekannter Quelle dürfen nicht geöffnet werden; sie müssen sofort gelöscht werden.

- E-Mail-Beilagen aus bekannten Quellen mit ausführbaren Anhängen wie **z.B. .exe, .bat, vbs**, etc. oder sonstigen unbekannten Endung dürfen **nicht** geöffnet werden; sie müssen sofort gelöscht werden.
- Bei Viren-Alarm durch den installierten Viren-Scanner muss die Arbeit sofort unterbrochen und der IT-Support gerufen werden; bis zur Entwarnung dürfen keine weiteren Aktivitäten an der entsprechenden Arbeitsstation vorgenommen werden.
- Bei Viren-Alarm auf Notebooks im Aussendienst, darf nach der Rückkehr ins Büro auf keinen Fall das entsprechende Gerät ohne vorherige Begutachtung durch den IT-Support an das Netzwerk von GSBR angeschlossen werden.
- Alle Benutzer des Netzwerkes vom GSBR sind zusätzlich aufgerufen, alle ihnen zur Verfügung stehenden Vorkehrungen zu treffen, um das Netzwerk vom GSBR von Computer-Viren freizuhalten.

XII. E-Mail und Internet

Das E-Mail-System ist für geschäftliche Zwecke eingerichtet worden. Eine zeitlich geringfügige private Nutzung von Internet und E-Mail wird toleriert. Durch die private Nutzung des Internetzuganges dürfen die Arbeitsleistung und die technische Infrastruktur nicht beeinträchtigt werden.

Die private Nutzung der GSBR-E-Mail-Adresse ist untersagt. Es gibt gratis E-Mail-Adressen wie GMX, Gmail, Bluewin etc.

Bei Ferien- und sonstigen Abwesenheiten ist jeder Benutzer verpflichtet, entweder die Abwesenheitsnotiz im E-Mail-Client (Outlook) zu aktivieren oder eine Stellvertretung zu organisieren (Stellvertreterfunktion im Outlook; keine direkte Weiterleitung).

Die automatische Weiterleitung von E-Mails an eine E-Mail-Adresse und ausserhalb des GSBR-Netzwerkes ist nicht erlaubt.

Jede unverschlüsselte E-Mail kann von jedermann abgefangen und eingesehen werden. Sensible Daten sollten deshalb extern nur über Inca Mail-E-Mail verschickt werden. Internes Netz ist geschützt.

Zum Schutz vor Spam-, Phishing- oder anderweitig schädlichen E-Mails wird bei GSBR eine E-Mail-Sicherheitslösung eingesetzt.

Das Aufrufen von Webseiten mit unsittlichen, erotischen, rassistischen, gewalttätigen oder gegen das geltende Recht verstossenden Inhalten ist untersagt.

Aus beweisrechtlichen Gründen wird der gesamte E-Mail-Verkehr revisionssicher aufgezeichnet. Hierbei werden geschäftliche und private E-Mails nicht unterschieden. Der Arbeitgeber GSBR ist berechtigt, bei Bedarf den aufgezeichneten E-Mail-Verkehr zu durchsuchen. Klar erkennbare private E-Mails dürfen vom Arbeitgeber nicht geöffnet werden. Alle anderen E-Mails dürfen nur mit Einwilligung und Beisein des entsprechenden Benutzers eingesehen werden.

Der gesamte Internetverkehr wird aufgezeichnet. Bei Verdacht auf Missbrauch des Internets (z.B. Verstoss gegen die Aufruf-Richtlinien) ist der Arbeitgeber berechtigt, die Aufzeichnungen zu kontrollieren. Er muss dabei aber die Einwilligung aller betroffenen Personen einholen.

Die Benutzer des GSBR-Netzwerkes sind von einer möglichen Aufzeichnung des E-Mail- und Internet-Verkehrs in Kenntnis gesetzt und akzeptieren diese Sicherheitsmassnahme.

XIII. Kalender in Outlook

Alle Benutzer sind verpflichtet, ihren Kalender im Outlook zu führen, damit jederzeit entsprechende Auskünfte erteilt werden können.

- Jeder geschäftsrelevante Termin muss eingetragen sein. Kein Eintrag im Kalender während der Arbeitszeit bedeutet, der Mitarbeitende ist verfügbar.
- Private Termine können falls gewünscht ebenfalls im Kalender eingepflegt werden. Mittels der Funktion «als privat kennzeichnen» lässt sich der Inhalt des Termins vor Dritten verbergen.

XIV. Social Media

Soziale Netzwerke und Plattformen wie Xing, Linkedin, Facebook, Youtube, Twitter sowie Foren und Blogs haben die Kommunikationswelt verändert. Auch GSBR bedient sich dieser sogenannten „Social Media" und vertritt hinsichtlich der Nutzung von Social Media durch die Mitarbeitenden eine liberale Haltung.

Für die private Nutzung von Social Media am Arbeitsplatz gelten die gleichen Regeln wie für die Internetnutzung. Die privaten Aktivitäten sind auf ein Minimum zu beschränken. Diese neuen Medien eröffnen vielerlei Chancen, bergen aber auch Risiken und Gefahren für Sie als Nutzer oder Betroffener sowie für GSBR. Da sich private und berufliche Nutzung von Social Media nicht immer trennen lässt, informieren wir über die wichtigsten Verhaltensregeln.

A. Wie ist mit Social Media umzugehen?

Behandle dein Gegenüber, wie du selbst behandelt werden möchtest. Vermeide erniedrigende, verletzende oder unwahre Äusserungen und verhalte dich auch professionell, wenn du Social Media privat nutzt. Prüfe deine Einträge sorgfältig, bevor du diese veröffentlichst – was einmal auf dem Netz ist, bleibt auch da.

Für den publizierten Inhalt auf Social Media ist jeder selbst verantwortlich und du kannst auch von Drittpersonen dafür belangt werden, durch straf- und zivilrechtliche Verfolgung sowie Schadenersatz. Du kannst dich auch nicht darauf berufen, dass getätigte Einträge oder aufgeschaltete Bilder in Foren oder Gruppen als nicht öffentlich gelten.

B. Worauf ist zu achten?

Ergänzend zum Personalreglement: Veröffentliche keine Aussagen, Kommentare, Dokumente oder Bilder, welche den GSBR schädigen könnten. Mach keine Aussagen im Namen vom GSBR, wenn du nicht dazu autorisiert wurdest. Geschäfts- oder rufschädigende Äusserungen, Drohungen und Beleidigungen über den GSBR, Arbeitskollegen, Vorgesetzte oder Dritte zu verbreiten sowie Äusserungen, die den Betriebsfrieden gefährden, sind unzulässig und können arbeitsrechtliche

Konsequenzen nach sich ziehen. Auch Mobbing-Handlungen, wie z.B. persönlichkeitsverletzende Äusserungen über Mitarbeitende in einer Facebook-Gruppe, sind zu unterlassen.

Wichtig ist, dass bei Veröffentlichungen Ihre Identität bekannt gegeben wird und beim GSBR relevanten Themen darauf aufmerksam wird, dass es sich um Ihre persönliche Meinung handelt.

C. Achtung: Urheberrechte!

Bei Videos, Bildern oder Texten ist besondere Vorsicht geboten, da deren Urheberrechte geklärt werden müssen. Berücksichtigung der Persönlichkeits- und Datenschutz der abgebildeten oder aufgeführten Personen (z.B. Arbeitskollegen oder Eventteilnehmer). Beachte, dass Einträge, Bilder oder Videomaterial in Social Media von Teilnehmern oder Freunden sehr einfach und schnell weitergeleitet werden und somit an eine breite Öffentlichkeit gelangen können.

D. Vertrauliches bleibt vertraulich!

Ergänzend zum Personalreglement: Sei achtsam im Umgang mit der Veröffentlichung von Geschäftsinformationen. Interne und vertrauliche Informationen, welche du im Rahmen deines Arbeitsverhältnisses erhältst, dürfen nicht verbreitet werden. Veröffentliche nichts über Dritte, sofern du nicht deren vorgängige Zustimmung erhalten hast. Im Zweifelsfall frag deinen Vorgesetzen oder verzichte auf die Veröffentlichung. Für die offizielle Kommunikation ist ausschliesslich die Geschäftsleitung befugt.

XV. Cloud Services

Für einen sicheren Umgang mit Cloud Services sind die Punkte in diesem Abschnitt zu befolgen:

- Cloud-Dienste jeglicher Art ersetzen bestehende offizielle GSBR IT-Services nicht.
- Dokumente, welche im Rahmen von Vorhaben/Projekten innerhalb eines Cloud-Dienstes erarbeitet werden, müssen nach Abschluss der solchen nach den bestehenden Vorgaben (revisionssicher) in den dafür vorgesehenen Ablageorten abgelegt/archiviert werden. Die Verantwortung hierzu trägt der/die Verfasser/in.
- Generell gilt: besonders schützenswerte Daten wie Personal-/Personendaten, Informationen wie z.B. Gesundheits- resp. Klienten Daten sowie auch Daten ohne Personenbezug jedoch mit hoher Vertraulichkeit zum Beispiel auf Grund von Geheimhaltungsvereinbarungen dürfen nicht in der Cloud gespeichert werden.
- Es gilt ferner, dass auch personenbezogene Daten von Kunden (Verträge, Aufträge, usw.) nicht in der Cloud gespeichert werden dürfen.
- Die Entscheidung, ob und unter welchen Bedingungen Daten in der Cloud bearbeitet werden dürfen, bestimmt der Schutzbedarf der solchen.
- Im Zweifelsfall darf ein Cloud-Dienst nicht verwendet werden sowie bleibt das Speichern von Daten auf nicht GSBR-Servern untersagt.
- Der Austausch von geschäftlichen Daten erfolgt entweder via Geschäfts-E-Mail oder Microsoft Teams - alle anderen Cloud-Dienste dürfen für geschäftliche Zwecke nicht genutzt werden.
- Die Freigabe auf Dokumente/Daten in der Cloud für den externen Zugriff ist untersagt.
- Die Rechtevergabe muss sorgfältig verwaltet werden, damit keine Daten in falsche Hände gelangen; nicht mehr benötigte Zugriffsrechte müssen wieder entfernt werden.

- Für den Zugang ist ein komplexes Passwort zu verwenden, das von Drittpersonen nicht erraten werden kann.
- Beim Öffnen von Dateien ist Vorsicht geboten, damit keine Viren in das GSBR-Netzwerk eingeschleust werden.

Wichtig: Bei Fragen und/oder Unklarheiten steht das GSBR-IT Team oder die Geschäftsleitung gerne zur Verfügung.

XVI. Abwesenheit eines Arbeitnehmers

Im Falle einer vorhersehbaren Abwesenheit eines Arbeitnehmers (z.B. Ferien, Militär usw.) muss der Absender einer Nachricht (insbesondere einer E-Mail) von der Abwesenheit und über die diesbezügliche Stellvertretungsregelung mittels Abwesenheitsnotiz informiert werden.

Ist ein Arbeitnehmer unerwartet während mehr als einem Arbeitstag abwesend und kann er trotz mehrmaligen Versuchen nicht erreicht werden, so darf eine vorgängig vom Arbeitnehmer bezeichnete Person seines Vertrauens oder an zweiter Stelle der Vorgesetzte unter Mithilfe der IT-Abteilung auf den dem betreffenden Arbeitnehmer zur Verfügung gestellten IT-Mitteln eine Abwesenheitsnotiz einrichten sowie auf die geschäftlichen Nachrichten des Arbeitnehmers zugreifen. Vom Inhalt privater Nachrichten darf keine Kenntnis genommen werden.

Der Arbeitnehmer gibt im Bedarfsfall zu diesem Vorgehen ausdrücklich sein Einverständnis und gibt seinem Vorgesetzten eine allfällige Person seines Vertrauens bekannt. Er kann sein Einverständnis jederzeit widerrufen oder seinem Vorgesetzten eine andere Person seines Vertrauens nennen.

XVII. Austritt eines Arbeitnehmers

Vor dem Austritt hat ein Arbeitnehmer sämtliche, die ihm vom GSBR zur Verfügung gestellten IT-Mittel dem Arbeitgeber abzugeben. Der austretende Arbeitnehmer hat spätestens zwei Wochen vor dem Austrittsdatum mit dem Nachfolger oder dem Vorgesetzten gemeinsam die E-Mailbox gesichtet und geschäftliche E-Mails auf dem Server für den Nachfolger abgelegt oder andernfalls an diesen weitergeleitet.

Die gilt auch für hängige betrieblichen Angelegenheiten, elektronischen Unterlagen und sonstige Nachrichten. Auch diese müssen der Nachfolgeperson oder dem Vorgesetzten weitergeleitet werden.

Bei Austritt sperrt der GSBR spätestens am letzten Arbeitstag die elektronischen Nachrichteneingänge als auch individualisierte Zugänge zu Software oder zu über das Internet oder Intranet verbundene Plattformen und Portale. Analog wird auch bei einem Todesfall eines Arbeitnehmers verfahren, wobei die bis zur Sperrung eingehenden Daten gespeichert werden.

Absender von Nachrichten an eine in diesem Sinne gesperrte Adresse, werden automatisch informiert, dass die Empfängeradresse hinfällig ist. In der automatischen Antwort wird eine geeignete Ersatz-Adresse dem *GSBR* angegeben.

XVIII. Sanktionierungen

Wird ein Verstoss gegen personalrechtliche Pflichten, geltende Gesetze oder die vorliegenden Benutzerrichtlinien festgestellt, können Rechte eingeschränkt (z.B. Internetzugang) und entsprechende Dateien mit privatem Inhalt nach Vorankündigung gelöscht werden. Vorbehalten bleiben die übrigen personalrechtlichen Sanktionsmöglichkeiten.

XIX. Schlussbestimmungen

Diese Benutzerrichtlinien treten per 1. Januar 2025 in Kraft.

Hiermit bestätige ich mit meiner Unterschrift die GSBR IT-Benutzerrichtlinien gelesen und verstanden zu haben, sowie akzeptiere ich die darin aufgeführten Bestimmungen uneingeschränkt.

Name: _____ Vorname: _____

Bereich: _____

Empfang bestätigt: _____ Datum: _____