SALZBURGER ABFALLBESEITIGUNG

REINHALTEVERBAND GROSSRAUM SALZBURG

Informationssicherheitsrichtlinie (NIS)

Soweit in dieser Richtlinie personenbezogene Bezeichnungen verwendet werden, richten sich diese an alle Geschlechter.

Dokument-Status: öffentlich
Version: 1.3
Gültig ab: 15.09.2025
Erstellt von: Dr. G. Dürnberger, Abteilung Recht
Genehmigt von: Mag. J. Weilhartner, LL. B. (KGF), Ing. St. Löcker (TGF)

1. Einleitung

Unsere Organisation verpflichtet sich, Strategien zu entwickeln und Maßnahmen zu implementieren, um die Verfügbarkeit unserer IT-Systeme zu gewährleisten, unerlaubten Zugriff zu verhindern und die unberechtigte Veränderung von Informationen zu vermeiden. Der Schutz vor externen Cyberangriffen und internen Bedrohungen steht im Mittelpunkt unserer Bemühungen.

2. Zweck und Anwendungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Partner und Dritte, die Zugriff auf unsere Informationssysteme und Daten haben. Sie soll sicherstellen, dass alle Informationen und IT-Systeme geschützt, verfügbar und integer sind.

3. Personenbezogene Daten

- Unter personenbezogenen Daten versteht man alle Informationen, die sich auf eine natürliche Person direkt oder indirekt beziehen und damit Rückschlüsse auf deren Persönlichkeit erlauben. Besonders schützenswerte personenbezogene Daten sind Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit.
- Die Verarbeitung und Weitergabe dieser Daten darf nur auf Grundlage der Art. 6 bis 11 DSGVO erfolgen.

4. Datenklassifizierung

Wir unterscheiden drei Typen von Daten und prüfen diese anhand der folgenden Kategorien:

- **Öffentliche Daten**: Alle Informationen, die vom Unternehmen im Rahmen einer gesetzlichen Berichtspflicht (Transparenzgebot/Offenlegungspflichten), wie z. B. Umweltdaten, statistische Daten, Jahresabschluss, Meldungen an das Firmenbuch, Bekanntgabepflichten nach dem MedientransparenzG und ParteienG, zu veröffentlichen sind, aber auch öffentliche Verwaltungsakte (z. B. Bescheide etc.).
- **Vertrauliche Daten**: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wie z.B. Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, SV-Nummer, Fotos etc., dürfen nur im Rahmen des Art. 6 der DSGVO verarbeitet werden. Sie unterliegen den strengen Datenschutzbestimmungen.
- **Geheime Daten**: Alle Informationen, die negative Auswirkungen auf die Organisation und Betriebswirtschaft des Unternehmens haben können, wie z.B. Schriftverkehr mit Kunden, Verträge, Finanzdaten, Gesundheitsdaten, strategische Pläne und interne Berichte/Protokolle, Sicherheitsinformationen (Passwörter, Zugangscodes).

5. Zugriff zu den einzelnen IT-Anwendungen

- Der Zugriff zu den einzelnen IT-Anwendungen ist über eine Zugriffskontrolle geregelt. Wer auf welche Daten zugreifen kann, ergibt sich aus den vom Administrator zugewiesenen Berechtigungen. Über die einzelnen Zugriffs-Berechtigungen entscheidet die Geschäftsführung bzw. Abteilungs- und Bereichsleiter.

6. Unsere Netzwerke und die verwendete Hardware

- Auf unseren betriebseigenen Netzwerken dürfen ausschließlich nur IT-Systeme betrieben werden, die durch die EDV-Betreuung geprüft wurden.
- Der Betrieb von systemfremder Hardware ist verboten.
- Die Weitergabe und die Umverteilung von Hardware unter den einzelnen Mitarbeitern erfolgen ausschließlich durch die EDV-Betreuung.

6.1 Notebooks/mobile Endgeräte

- Der Mitarbeiter hat Notebooks und mobile Endgeräte pfleglich zu behandeln und dafür zu sorgen, dass das Gerät sicher verwahrt und nicht von Unbefugten benutzt werden kann.
- Besonders schützenswerte Firmendaten (vertrauliche und geheime Daten) dürfen nicht auf dem Notebook gespeichert werden, sofern das Gerät nicht mit Festplattenverschlüsselung ausgestattet ist.
- Diebstahl, Verlust oder Beschädigung sind unverzüglich der EDV-Betreuung zu melden.
- Die Nutzung privater Cloud-Speicher für Unternehmensdaten ist verboten.
- Die Nutzung privater mobiler Endgeräte für betriebliche Zwecke (siehe die BYOD-Richtlinie in der jeweils aktuellen Fassung) ist nur nach vorheriger Genehmigung durch die Geschäftsführung erlaubt.

6.2 Netzwerkanschluss

- Der Anschluss von Hardware an das Netzwerk darf nur durch die EDV-Betreuung erfolgen.
- Es ist verboten, selbstständig Hardware an das Netzwerk an- bzw. abzuschließen. Dies gilt auch und insbesondere für Notebooks von Gästen, denen ein Gäste-WLAN zur Verfügung steht.

7. Software

7.1 Anschaffungen von Software

- Die Anschaffung von Software wird ausschließlich nach Freigabe durch die Geschäftsführung durchgeführt.
- Für den Einsatz der Software werden in allen Bereichen des Unternehmens entsprechende Software-Lizenzen benötigt.
- Die Verwendung von nicht durch das Unternehmen erworbener Software sowie von Software ohne gültige Lizenz ist verboten.

7.2 Software-Installation

- Die Mitarbeiter sind nicht zur Installation von Software auf den benutzten Endgeräten berechtigt. Für Private Endgeräte siehe die „Mobile Device Richtlinie".
- Die Nutzung von Software (auch das Starten von Anwendungen ohne Installation), die nicht durch die EDV-Bereuung geprüft und durch die Geschäftsführung freigegeben wurde, ist verboten.

8. Passwörter

- Der Zugriff auf die IT-Systeme ist durch Benutzerkonten mit Passwort gesichert. Auf die Passwortrichtlinie in der aktuellen Fassung wird verwiesen.
- Die Zugangsdaten für Web-Portale oder sonstige Dienste, die eine Autorisierung vorsehen, sind in sicherer Form zu speichern.
- Es ist untersagt, mit einem fremden Benutzerprofil zu arbeiten, es sei denn, es handelt sich um ein allgemeines Benutzerkonto, welches speziell für diesen Zweck freigegeben wurde.
- Es ist darauf zu achten, wer in den Bildschirm einsehen kann.

9. Verhalten am Arbeitsplatz

- Beim Verlassen des Arbeitsplatzes ist die Bildschirmsperre (Bildschirmschoner) zu aktivieren oder eine Systemabmeldung durchzuführen.
- Wird der Arbeitsplatz für längere Zeit verlassen (z. B. Arbeitsschluss, Dienstreise etc.) ist der PC bzw. das Notebook herunterzufahren oder in den Ruhezustand zu versetzen und abzusperren.
- Es ist darauf zu achten, dass unberechtigte Personen (z. B. Reinigungspersonal, unbefugte Mitarbeiter oder Besucher) keinen Zugriff auf vertrauliche Dokumente/Informationen haben.
- Netzwerkdrucker und -scanner dürfen nicht abgeschaltet werden.
- Im Abwesenheitsfall soll der Mitarbeiter möglichst eine Abwesenheitsnachricht einrichten.

10. E-Mail, Web

- Der Internetzugang und das E-Mail-System werden für die dienstliche Nutzung zur Verfügung gestellt, eine private Nutzung ist auf ein Minimum zu beschränken.
- Der Mitarbeiter ist verpflichtet, eingehende E-Mails mit äußerster Sorgfalt zu prüfen.
- E-Mails, die in Bezug auf Absender, Betreffzeile und/oder Dateianhang verdächtig erscheinen, sind sofort zu löschen. Keinesfalls darf ein verdächtiger Anhang vom Mitarbeiter selbst geöffnet werden. Eine Meldung von Spam-Mails an die EDV-Betreuung hat nur zu erfolgen, wenn der Verdacht besteht, dass mehrere Personen im Unternehmen von der Spam-Mail betroffen sein könnten bzw. wenn ein gewisses Gefahrenpotenzial vermutet wird.
- Private E-Mails sind von Beschäftigten nach Kenntnisnahme des privaten Charakters unverzüglich zu löschen.
- Das Downloaden von ausführbaren Programmen (exe-Datei) aus dem Internet sowie das Ausführen von Bildschirmschonern und anderen Programmen, die als Attachments zu E-Mails empfangen werden, sind aus Sicherheitsgründen (Viren, Würmer, etc.) verboten.
- Der Versand von Dokumenten mit vertraulichem oder kritischem Inhalt muss entsprechend sensibel erfolgen.
- E-Mails, für die aufgrund ihres Inhalts gesetzliche Aufbewahrungsfristen gelten, müssen für eben diesen Zeitraum gespeichert werden.
- Bei Ausscheiden eines Mitarbeiters ist das Unternehmen berechtigt, eine Weiterleitung von E-Mails bei Abwesenheit und/oder einen Zugriff auf empfangene bzw. versandte betriebliche E-Mails einzurichten, wenn dies für betriebliche Zwecke erforderlich ist. Der Mitarbeiter muss damit rechnen, dass dadurch auch private E-Mails versehentlich gelesen werden können.
- Mit Beendigung des Beschäftigungsverhältnisses steht die E-Mail-Adresse des jeweiligen Mitarbeiters nicht mehr für diesen zur weiteren Nutzung zur Verfügung. Die Mitarbeiter sind angehalten, ihre außerbetrieblichen Kommunikationspartner über diesen Umstand zu informieren.

11. Abwehr von Schadprogrammen (Firewall/Virenschutz)

- Auf jedem Endgerät ist die Abwehr von Schadprogrammen (z. B. durch Firewall und/oder Virenschutz) sicherzustellen.
- Es ist verboten, installierte Abwehr-Tools zu deaktivieren oder zu deinstallieren.
- Bei jedem Virenverdacht auf dem Datenbestand ist sofort der Notfallmanager zu verständigen. Der Versuch, das Virus selbst zu löschen, ist zu unterlassen. Auf den IT-Notfallplan in der aktuellen Fassung wird verwiesen (siehe Aushang).

12. Datenspeicherung/-sicherung, Datenträger

- Die automatische Datensicherung erfolgt auf dem jeweiligen Netzlaufwerk, das dem Mitarbeiter zugewiesen ist.
- Für Daten, die auf lokalen Festplatten und Geräten gespeichert wurden, kann die Sicherheit nicht gewährleistet werden. Aus diesem Grund werden alle Mitarbeiter ausdrücklich angewiesen, firmenrelevante Informationen ausschließlich auf den zugewiesenen Netzwerklaufwerken zu speichern.

- Das Speichern von privaten Daten ist verboten.
- Für den Austausch von Daten sind ausschließlich die vom Unternehmen zur Verfügung gestellten Speicher- und Übertragungsmedien zu verwenden.
- Der Einsatz von externen physischen Datenträgern und von Übertragungsmechanismen (wie z. B. Bluetooth, WLAN etc.) hat mit äußerster Zurückhaltung zu erfolgen.
- Um die Sicherheit von besonders schützenswerten Daten zu gewährleisten, wird der Einsatz einer Zwei-Faktor-Authentifizierung empfohlen.
- Der Mitarbeiter ist verpflichtet, jederzeit den korrekten Drucker zu verwenden und ausgedruckte vertrauliche Informationen umgehend aus dem Drucker zu entfernen.
- Sämtliche Datenträger (USB-Stick, Festplatte, SD-Karte, CD/DVD etc.) müssen am Ende ihrer Nutzungsdauer entsorgt werden. Ein entsprechender Entsorgungsnachweis ist an die EDV-Betreuung zu übergeben.

13. Anwendung auf Mobiltelefone

- Die Vorschriften dieser Richtlinie gelten - soweit anwendbar - auch für mobile Geräte, die vom Unternehmen dem Mitarbeiter zur Verfügung gestellt werden, oder private Geräte, die der Mitarbeiter nach Genehmigung der Geschäftsführung für dienstliche Zwecke verwendet, insbesondere für Mobiltelefone.
- Der Mitarbeiter ist dafür verantwortlich, dass seine Nutzung die Freieinheiten des für ihn freigeschalteten Tarifs nicht übersteigt.
- Sofern sich der Mitarbeiter im Ausland aufhält, ist er verpflichtet, rechtzeitig vor Abreise von der IT-Abteilung passende Pakete freischalten zu lassen.
- Bei Verlust bzw. Diebstahl des Mobiltelefons ist unverzüglich die EDV-Betreuung zu verständigen, damit das Mobiltelefon gesperrt werden kann.

14. Änderungsmanagement

Änderungen dieser Richtlinie werden durch die EDV-Betreuung initiiert und müssen durch die Geschäftsführung genehmigt werden. Alle Mitarbeiter werden durch Aushang über diese Richtlinie in Kenntnis gesetzt. Alle Mitarbeiter werden über Änderungen informiert und geschult.

15. Schlussbestimmungen

Diese Richtlinie tritt mit sofortiger Wirkung in Kraft und wird regelmäßig - mindestens jedoch einmal im Jahr - überprüft und bei Bedarf aktualisiert. Verstöße gegen diese Richtlinie können disziplinarische Maßnahmen nach sich ziehen, einschließlich der Kündigung.

Bergheim, am 10.9.2025

Die Geschäftsführung:

Mag. J. Weilhartner, LL. B.(KGF)

Ing. St. Löcker (TGF)

Verteiler: KGF, TGF, PR, RC, alle AL SAB GmbH und RHV, TKO, EDV-Betreuung, Systemadministratoren, Datenschutzbeauftragter, Betriebsrat Arb.-SAB, Betriebsrat Ang.-SAB, Betriebsrat Arb.-RHV.