Vertragliche Informationssicherheitsrichtlinien für externe IT-Dienstleistungen und Systemnutzung

1 Einleitung und Geltungsbereich

Die Unternehmen der GASAG-Gruppe beauftragen externe Unternehmen (nachfolgend Dienstleister) zur Erbringung von IT-bezogenen Dienstleistungen. Die Nutzung von IT-Systemen und der Zugriff auf Daten der GASAG-Gruppe durch diese Dienstleister erfordert die Einhaltung spezifischer Anforderungen zur Gewährleistung der Informationssicherheit und des Datenschutzes. Dieses Dokument fasst die vertraglichen und technischen Sicherheitsanforderungen zusammen und stellt die verbindliche Grundlage für jede Zusammenarbeit dar.

Diese Anforderungen gelten für sämtliche externen Dienstleister, die in irgendeiner Form mit IT-Systemen, Daten oder Netzwerken der GASAG-Gruppe interagieren. Sie basieren auf dem NIST Cybersecurity Framework (CSF) 2.0 sowie den relevanten Anforderungen der ISO/IEC 27001:2022. Ziel ist es, ein einheitliches Sicherheitsniveau zu etablieren und systemische Risiken frühzeitig zu erkennen, zu minimieren und im Ereignisfall effektiv zu bewältigen.

2 Organisatorische und vertragliche Grundanforderungen

Der Dienstleister trägt die volle Verantwortung für die Sicherheit aller eingesetzten Systeme und Prozesse im Rahmen der Auftragsdurchführung.

Zugriffsrechte sind nach dem Need-to-know-Prinzip restriktiv zu vergeben, regelmäßig zu überprüfen und nachvollziehbar zu dokumentieren. Der Zugriff auf Systeme und Daten ist ausschließlich autorisierten Personen gestattet.

Schulungen zur Informationssicherheit sind regelmäßig durchzuführen, um das Sicherheitsbewusstsein der Mitarbeitenden aufrechtzuerhalten und aktuelle Bedrohungen adressieren zu können.

Eine Speicherung oder Weitergabe von Daten der GASAG-Gruppe ist nur mit ausdrücklicher schriftlicher Genehmigung zulässig.

Die Nutzung mobiler Datenträger, automatisierte E-Mail-Weiterleitungen sowie die private Nutzung von Systemen oder Informationen sind untersagt.

Alle Systeme sind regelmäßig zu aktualisieren. Sicherheitslücken sind umgehend zu melden. Neuinstallationen oder Konfigurationsänderungen dürfen nur in Abstimmung mit der GASAG-Gruppe erfolgen.

Die GASAG-Gruppe behält sich vor, technische Prüfungen und Protokollierungen durchzuführen.

Nach Beendigung des Auftrags sind sämtliche Zugänge zu deaktivieren und ausgegebene Geräte vollständig zurückzugeben.

3 Technische Sicherheitsanforderungen

3.1 Identify (Identifizieren)

Der IT-Dienstleister ist verpflichtet, ein vollständiges und regelmäßig gepflegtes IT-Asset-Management zu betreiben. Es muss alle relevanten Komponenten umfassen – darunter stationäre und mobile Endgeräte, Server, Software, virtuelle Maschinen sowie Cloud-Dienste. Ziel ist ein jederzeit verlässlicher Überblick über eingesetzte Systeme und deren Sicherheitsstatus.

Alle im Rahmen der Leistungserbringung verarbeiteten Informationen sind nach Schutzbedarf zu klassifizieren. Vertrauliche und personenbezogene Daten müssen eindeutig identifiziert und entsprechend gekennzeichnet werden, um deren Schutz über den gesamten Lebenszyklus hinweg sicherzustellen.

Der Dienstleister führt regelmäßig strukturierte Risikoanalysen durch. Diese beinhalten unter anderem Threat Modeling, Business Impact Assessments sowie Penetrationstests. Die Ergebnisse sind in angemessene Schutzmaßnahmen zu überführen.

Eingesetzte Dritte oder Unterauftragnehmer sind auf Basis klarer Sicherheitsanforderungen auszuwählen, zu bewerten und regelmäßig zu überwachen. Die Verantwortung für deren Sicherheitsleistung verbleibt beim Dienstleister.

Ein aktives Schwachstellenmanagement ist zu betreiben. Kritische Sicherheitslücken müssen spätestens innerhalb von 14 Kalendertagen nach Bekanntwerden wirksam behoben werden.

3.2 Protect (Schützen)

3.2.1 Netzwerksicherheit:

Der IT-Dienstleister hat sicherzustellen, dass alle Systeme konsequent dem Zero-Trust-Prinzip folgen. Jeder Zugriff muss strikt authentifiziert und autorisiert werden – unabhängig von Nutzer, Gerät oder Standort. Vertrauen entsteht nicht automatisch, sondern wird durch technische Maßnahmen kontinuierlich überprüft.

Zum Schutz der internen Infrastruktur sind moderne Sicherheitslösungen einzusetzen. Dazu gehören Firewalls mit integrierten Intrusion Detection- und Prevention-Systemen (IDS/IPS) sowie eine konsequente Segmentierung des Netzwerks. Die Konfigurationen dieser Systeme sind mindestens vierteljährlich zu prüfen und bei Bedarf anzupassen, um veränderten Bedrohungslagen Rechnung zu tragen.

Der ausgehende Datenverkehr (Outbound-Traffic) ist klar zu reglementieren und ausschließlich auf genehmigte Geschäftsprozesse zu beschränken. Dadurch wird das Risiko unerwünschter Datenabflüsse oder Kommunikationsverbindungen signifikant reduziert.

3.2.2 VPN & Remote Access

Fernzugriffe durch externe Dienstleister müssen über sichere und verschlüsselte Kommunikationsmethoden erfolgen. Die eingesetzten Verfahren müssen den aktuellen Stand der Technik erfüllen und gewährleisten, dass Datenintegrität, Vertraulichkeit und Authentizität sichergestellt sind.

Grundprinzipien

- **Verschlüsselung:** Alle Datenübertragungen müssen durch starke Verschlüsselung abgesichert sein (z. B. TLS, IPSec).
- **Authentifizierung:** Zugriff darf nur nach erfolgreicher Authentifizierung erfolgen, vorzugsweise mit Multi-Faktor-Authentifizierung (MFA).
- **Zugriffsbegrenzung:** Dienstleister erhalten nur Zugriff auf die für ihre Tätigkeit erforderlichen Systeme und Ressourcen.
- **Sichere Zugriffsmethoden:** Beispiele für zulässige Methoden:
    - VPN-Verbindungen (IKEv2/IPSec, SSL VPN) für nicht-öffentliche Systeme.
    - HTTPS/TLS für Cloud-Dienste wie Microsoft 365.
    - Gleichwertige sichere Zugriffsdienste (z. B. Azure Bastion für VMs).
- **Unsichere Protokolle** (z. B. unverschlüsseltes RDP, FTP) sind verboten.

Ausnahmen und Klarstellungen

- Für Cloud-Dienste, die bereits durch TLS und Azure AD-Mechanismen abgesichert sind (z. B. Microsoft 365, Teams, SharePoint), ist keine zusätzliche VPN-Verbindung erforderlich.
- Für virtuelle Maschinen oder andere IaaS-Ressourcen muss eine sichere Zugriffsmethode wie VPN oder Azure Bastion genutzt werden.

Der Einsatz von Split-Tunneling – also die gleichzeitige Nutzung des VPNs und direkter Internetverbindungen – ist grundsätzlich untersagt. Ausnahmen bedürfen einer ausdrücklichen Genehmigung sowie technischer und organisatorischer Zusatzmaßnahmen zur Risikominderung.

Zur Nachvollziehbarkeit und Sicherheitsüberwachung sind VPN-Verbindungsdaten (z. B. Nutzerkennung, Zeitpunkt, genutzte Ressourcen) für mindestens 90 Tage revisionssicher zu protokollieren.

3.2.3 E-Mail-Sicherheit:

Zur Absicherung der E-Mail-Kommunikation sind geeignete technische und organisatorische Maßnahmen verpflichtend einzusetzen, die den aktuellen Stand der Technik erfüllen. Ziel ist die Sicherstellung von Vertraulichkeit, Integrität und Authentizität der Kommunikation sowie der Schutz vor Schadsoftware und Phishing-Angriffen.

Grundprinzipien

- **Authentifizierung und Anti-Spoofing:** Mechanismen zur Überprüfung der Absenderidentität müssen implementiert sein (z. B. SPF, DKIM, DMARC oder gleichwertige Verfahren).
- **Mehrschichtige Bedrohungsabwehr:** Einsatz von leistungsfähigen E-Mail-Gateways mit integrierter Malware- und Spam-Filterung sowie erweiterten Schutzmechanismen gegen Phishing und Schadsoftware (z. B. Advanced Threat Protection oder vergleichbare Lösungen).

- **Quarantäne für kritische Inhalte:** Eingehende E-Mails mit potenziell gefährlichen Anhängen müssen in eine Quarantäne verschoben werden, die eine manuelle Prüfung und Freigabe durch berechtigte Personen ermöglicht.
- **Verschlüsselte Übertragung:** Alle E-Mail-Verbindungen müssen durch aktuelle Verschlüsselungsstandards (z. B. TLS) abgesichert sein.
- **Organisatorische Maßnahmen:** Regelmäßige Schulungen für Mitarbeitende sind verpflichtend, einschließlich simulierten Phishing-Kampagnen zur Stärkung des Sicherheitsbewusstseins.
- **Weiterleitungsbeschränkung:** Die automatische Weiterleitung eingehender E-Mails an externe Empfänger ist grundsätzlich untersagt, da sie ein erhebliches Sicherheitsrisiko darstellt.

3.2.4 Endpunktschutz:

Alle eingesetzten Endgeräte müssen mit einer aktuellen Endpoint Detection & Response (EDR)-Lösung ausgestattet sein. Diese Lösung muss zentral verwaltbar sein, um einheitliche Sicherheitsrichtlinien durchzusetzen und Bedrohungen frühzeitig zu erkennen.

Es dürfen ausschließlich durch die GASAG-Gruppe freigegebene Systeme verwendet werden. Die Nutzung abweichender Hard- oder Softwarekonfigurationen ist untersagt, sofern keine ausdrückliche Genehmigung vorliegt.

Lokale Administratorrechte für die Systeme der GASAG-Gruppe sind grundsätzlich nicht zulässig. Ausnahmen gelten nur für eindeutig definierte systemadministrative Rollen und müssen dokumentiert und regelmäßig überprüft werden.

Zum sicheren Umgang mit lokalen Administratorkonten ist die Einführung von Microsoft LAPS oder einer vergleichbaren Lösung für das automatisierte und geschützte Passwortmanagement verpflichtend.

Ein wirksames Patch-Management ist sicherzustellen: Kritische Sicherheitsupdates müssen spätestens innerhalb von 14 Tagen installiert werden, alle übrigen Updates sind monatlich einzuspielen.

3.2.5 Datenträgereinsatz:

Der Einsatz externer USB-Geräte ist streng zu reglementieren. Es dürfen ausschließlich zuvor genehmigte und automatisch verschlüsselte Speichermedien verwendet werden. Dies dient dem Schutz vor unautorisiertem Datenabfluss sowie dem Einschleusen schädlicher Software.

Automatische Startfunktionen (Autorun) sind auf allen Endgeräten dauerhaft zu deaktivieren, um potenzielle Sicherheitsrisiken durch manipulierte Datenträger zu minimieren.

Dateiübertragungen auf oder von externen Medien sind lückenlos zu protokollieren. Zusätzlich sind geeignete DLP-Technologien (Data Loss Prevention) oder gleichwertige Lösungen einzusetzen, um sensible Daten vor unbeabsichtigtem Abfluss zu schützen.

3.2.6 Verschlüsselung:

Sämtliche Daten – sowohl im Ruhezustand (at rest) als auch während der Übertragung (in transit) – sind durch angemessene kryptografische Verfahren zu schützen. Dabei sind mindestens AES-256 für gespeicherte Daten und TLS 1.2 oder höher für die Übertragung zu verwenden, um den aktuellen Sicherheitsanforderungen zu entsprechen.

Für die Verwaltung kryptografischer Schlüssel wird der Einsatz von Hardware Security Modules (HSMs) empfohlen. Diese bieten ein hohes Maß an Schutz vor unbefugtem Zugriff und tragen zur sicheren, zentralen Schlüsselverwaltung bei.

3.2.7 Zugriffsmanagement:

Die Nutzung moderner, passwortloser Authentifizierungsverfahren – wie FIDO2, Smartcards oder biometrischer Verfahren – wird ausdrücklich empfohlen, da sie ein höheres Sicherheitsniveau und bessere Nutzerfreundlichkeit bieten.
Für den Zugriff auf kritische Systeme sind SSO-Lösungen (Single Sign-On) mit verpflichtender Multi-Faktor-Authentifizierung (MFA) einzusetzen. Dadurch wird sichergestellt, dass nur berechtigte Nutzer unter Einbindung eines zweiten Faktors auf sensible Ressourcen zugreifen können.

Die Vergabe von Zugriffsrechten hat auf Basis eines rollenbasierten Zugriffskontrollmodells (RBAC) zu erfolgen. Hierbei ist sicherzustellen, dass jeder Nutzer nur Zugriff auf die Systeme und Informationen erhält, die für seine Aufgaben erforderlich sind (Prinzip der minimalen Rechtevergabe).

Inaktive Konten sind mindestens monatlich zu identifizieren und zu deaktivieren. Privilegierte Konten müssen mindestens alle sechs Monate im Rahmen einer Rezertifizierung überprüft und dokumentiert freigegeben werden.

3.3 Detect (Erkennen)

Zur frühzeitigen Erkennung sicherheitsrelevanter Vorfälle sind alle relevanten Logdaten zentral in ein Security Information and Event Management (SIEM)-System zu integrieren. Die Daten sind dort mindestens 12 Monate lang revisionssicher aufzubewahren.

Das System muss in der Lage sein, sicherheitskritische Ereignisse wie wiederholte fehlgeschlagene Anmeldeversuche, Änderungen an Firewall-Regeln oder unautorisierte Eskalationen von Benutzerrechten automatisiert zu erkennen und zu melden.

Für besonders schützenswerte oder unternehmenskritische Systeme ist eine kontinuierliche Echtzeitüberwachung verpflichtend, um Angriffsversuche oder technische Anomalien unmittelbar zu identifizieren und Gegenmaßnahmen einzuleiten.

3.4 Respond (Reagieren)

Der Dienstleister muss über einen strukturierten und dokumentierten Incident-Response-Plan verfügen. Dieser ist regelmäßig zu aktualisieren und mit der GASAG-Gruppe abzustimmen, um eine koordinierte Reaktion auf Sicherheitsvorfälle zu gewährleisten.

Sicherheitsvorfälle sind unverzüglich, spätestens jedoch innerhalb von 24 Stunden, an die definierten Meldestellen informationssicherheit@gasag.de und itsm@gasag.de zu berichten.

Zur Vorbereitung auf reale Vorfälle sind regelmäßig Schulungen und sogenannte Tabletop-Übungen durchzuführen, um Rollen, Abläufe und Kommunikationswege im Notfall zu erproben.

Kritische Sicherheitsvorfälle sind im Nachgang systematisch aufzuarbeiten. Dazu gehört die Durchführung eines dokumentierten „Post-Mortem“, um Ursachen, Auswirkungen und Optimierungspotenziale zu identifizieren.

3.5 Recover (Wiederherstellen)

Zur Sicherstellung der Wiederherstellbarkeit von Systemen und Daten sind regelmäßig vollständige Backups zu erstellen. Diese müssen offline gespeichert werden – beispielsweise als air-gapped oder immutable Kopien – um sie vor Manipulation oder Verschlüsselung durch Schadsoftware zu schützen. Die Wiederherstellung aus den Sicherungen ist regelmäßig zu testen und zu dokumentieren, um ihre Verlässlichkeit im Ernstfall sicherzustellen.

Für den IT-Betrieb sind Notfallpläne vorzuhalten, die mindestens einmal jährlich überprüft, bei Bedarf aktualisiert und in Form von Übungen praktisch erprobt werden müssen. Ziel ist die Aufrechterhaltung oder schnelle Wiederherstellung der Betriebsfähigkeit bei gravierenden Störungen.

Nach schwerwiegenden Sicherheits- oder Systemvorfällen sind strukturierte Lessons-Learned-Workshops durchzuführen. Dabei sollen Ursachen analysiert, Schwachstellen identifiziert und Verbesserungsmaßnahmen abgeleitet werden.

4 Ausführungsort und Zugriffsbeschränkung außerhalb des EWR-Raums

Der Dienstleister verpflichtet sich, sämtliche im Rahmen dieses Vertrags beauftragten Leistungen ausschließlich innerhalb des Gebietes der Europäischen Union sowie in Norwegen, Island, Liechtenstein und der Schweiz zu erbringen. Eine Erbringung oder (teilweise) Ausführung der Leistungen aus anderen Staaten ist unzulässig, es sei denn, der Auftraggeber erteilt hierzu eine ausdrückliche, schriftliche Genehmigung.

Der Dienstleister hat organisatorische und technische Maßnahmen zu implementieren, um Zugriffe aus nicht autorisierten Ländern präventiv zu verhindern (z. B. IP-Geofencing, Netzwerksegmentierung, VPN-Beschränkung nach Region). Diese Maßnahmen sind nach dem Stand der Technik und unter Berücksichtigung etablierter Standards (z. B. ISO/IEC 27001, NIS2, BSI IT-Grundschutz) umzusetzen.

Der Zugriff auf Systeme, Anwendungen oder Daten der GASAG-Gruppe aus Ländern außerhalb der genannten Gebiete ist strikt untersagt – unabhängig davon, ob dieser durch Mitarbeitende des Dienstleisters, durch Subunternehmer oder sonstige Dritte erfolgt. Dieses Verbot gilt insbesondere für Remote-Zugriffe aus sogenannten Drittstaaten im Sinne der DSGVO.

5 Zentrale Ansprechpartner

Als Dienstleister der GASAG-Gruppe benennt dieser mit Aufnahme der Tätigkeit eine Kontaktstelle für alle Belange der Informationssicherheit. Die vollständigen Kontaktdaten sind an das Postfach informationssicherheit@gasag.de zu senden.

6 Sicherheitsüberprüfung

Die GASAG-Gruppe ist berechtigt, in Bezug auf die vom Dienstleister erbrachten Leistungen, technische Überprüfungen aller Sicherheitsaspekte durchzuführen. Der Dienstleister verpflichtet sich zur Mitwirkung.

7 Verfügbarkeit

Die GASAG-Gruppe kann Zugänge ohne Nennung von Gründen und ohne in Kenntnissetzung des Dienstleisters aussetzen, sofern die Sicherheit der GASAG-Gruppe gefährdet ist.

8 Beginn/Beendigung

Zugriffe werden durch die GASAG-Gruppe bereitgestellt, sobald alle Voraussetzungen erfüllt sind. Die erteilten Zugriffe enden spätestens bei Auslaufen des Vertrages. Bei Beendigung der Vertragsverhältnisse gibt der Dienstleister innerhalb von 10 Werktagen alle Geräte zurück, die ggf. zur Ermöglichung des Fernzugriffs von der GASAG-Gruppe bereitgestellt wurden.

9 Haftung

Die GASAG-Gruppe übernimmt keine Verantwortung für Verluste, Schäden oder Kosten, die dem Dienstleister direkt oder indirekt durch die Nutzung oder Nicht-Verfügbarkeit des Fernzugriffs entstehen. Bei Verstößen gegen rechtliche Bestimmungen ist der Dienstleister für alle direkten und indirekten Verluste, Schäden und Kosten, die der GASAG-Gruppe entstehen, haftbar. Eine solche Haftung schließt jedoch weder andere Ansprüche aus noch stellt sie eine Außerkraftsetzung der GASAG-Gruppe per Gesetz oder anderweitig zustehender Rechte und Rechtsmittel dar.

Im Falle eines Sicherheitsvorfalls, der auf Fahrlässigkeit oder Nichtbefolgung der hier festgelegten Sicherheitsstandards zurückzuführen ist, haftet der Dienstleister für alle entstehenden direkten und indirekten Schäden.

10 Rechtsverbindlichkeit und Maßnahmen bei Zuwiderhandlung

Diese Sicherheitsanforderungen sind verbindlich einzuhalten. Verstöße können zur sofortigen Suspendierung der Zugänge sowie zur Beendigung der Zusammenarbeit führen. Ergänzend gelten alle bestehenden Sicherheits- und Datenschutzrichtlinien der GASAG-Gruppe.

Die vollständige oder teilweise Ungültigkeit von Punkten dieser Vertragsanlage beeinträchtigt nicht die Gültigkeit der anderen Punkte. Änderungen dieses Dokumentes sowie ergänzende Bestimmungen, einschließlich der in diesem Punkt festgelegten Anforderung, bedürfen der Schriftform; wobei Schriftform durch eine einfache beidseitige elektronische Signatur mittels DocuSign ersetzt werden kann.