Richtlinie für vertraglich gebundene externe Nutzer der GASAG Konzern-IT-Systeme

Fachverantwortlicher:		IT-Konzernstrategie	
Version	1.0	**Letzte Aktualisierung:**	16.03.2009

Inhaltsverzeichnis

1 Geltungsbereich

Die Unternehmen der GASAG-Gruppe beauftragen zur Erbringung von IT-Services (Beratung, Anwendungsentwicklung und Betrieb) externe/konzernfremde IT-Dienstleister. Die dafür erforderliche Nutzung von Konzern-IT-Systemen der GASAG-Gruppe durch externe Anwender unterliegt den hier dargestellten Voraussetzungen. Diese sind als Mindestanforderung für eine Dienstleistungserbringung zu verstehen. Soweit diese Mindestanforderungen durch den IT-Dienstleister nicht erfüllt werden können, ist eine Zusammenarbeit mit Unternehmen der GASAG-Gruppe ausgeschlossen.

2 Persönliche Verantwortung

Externe Benutzer sind selbst für ihre eigene Informationsverarbeitung verantwortlich, die den in der vorliegenden Richtlinie festgelegten Regelungen zu folgen hat. Potenzielle Verstöße gegen die Festlegungen der vorliegenden Richtlinie können die Verhängung einer Pönale oder gesetzliche Schadenersatzforderungen nach sich ziehen.

- Voraussetzung zur Nutzung der GASAG Konzern-IT-Systeme ist die durch die Stabsstelle IT-Konzernstrategie oder weitere berechtigte Mitarbeiter des Konzerns ausdrücklich erteilte Berechtigung.

- Die Berechtigung zur Nutzung der GASAG Konzern-IT-Systeme ist personengebunden und nicht übertragbar.

- Die Voraussetzungen der entsprechenden Berechtigung zur Nutzung der IT-Systeme, sowie urheberrechtliche, patentrechtliche Bestimmungen sowie Lizenzvereinbarungen über Software und einschlägige gesetzliche Bestimmungen sind einzuhalten.

- Der Dienstleister hat jederzeit sicher zu stellen, dass sein Handlungen nicht die Verfügbarkeit, Integrität oder Vertraulichkeit von IT-Systemen beeinträchtigen.

3 Nutzung von IT-Systemen

Es obliegt dem externen Vertragspartner sicherzustellen, dass ausschließlich mit der Auftragsbearbeitung betraute und sachkundige Personen Zugang zu den Daten des GASAG-Konzerns gemäß der vorliegenden Richtlinie erhalten. Der Lieferant ist für die Handlungen oder Unterlassungen seiner Nachauftragnehmer auf die gleiche Weise wie für seine eigenen Handlungen oder Unterlassungen verantwortlich.

- Die erteilten Zugriffsberechtigungen und/oder die Verwendung personenbezogener und anderer betrieblicher Daten dienen ausschließlich der Erfüllung des Vertragsgegenstandes.

- Daten des GASAG-Konzerns sind ausschließlich auf den bereitgestellten IT-Systemen zu verarbeiten. Ausnahmen erfordern eine gesonderte Genehmigung durch die Stabsstelle IT-Konzernstrategie.

- Sicherheitsrelevante Konfigurationen sind generell nicht zu ändern oder außer Kraft zu setzen.

- Jeder Nutzer ist mitverantwortlich dafür, bei seiner täglichen Arbeit für die Sicherheit der IT-Systeme zu sorgen.

3.1 Zugriffsschutz

- Sichern Sie die Informationssysteme im Rahmen Ihrer Möglichkeiten gegen den Zugriff durch Unbefugte.
- Sperren Sie die Informationssysteme, wenn Sie diese nicht nutzen.
- Vorgegebene Initial-Passwörter sind durch ein der Kennwortkomplexitätsrichtlinie genügendes Passwort zu ersetzen.
- Behandeln Sie Ihr Passwort vertraulich und teilen Sie es niemandem mit.
- Für Ihre Adresse / Ihr Konto ebenso wie für Ihr Passwort sind Sie selbst verantwortlich.

3.2 Datenschutz

- Die Übertragung von Daten des GASAG-Konzerns an Dritte ist nicht zulässig. Ausnahmen erfordern eine gesonderte Genehmigung.
- Sämtlicher E-Mail-Verkehr zwischen dem GASAG-Konzern und dem Auftragnehmer ist angemessen vertraulich zu behandeln.
- Das Speichern von Daten des GASAG-Konzerns in unverschlüsselter Form ist auf mobilen Datenträgern (z.B. USB-Sticks) unzulässig. Ausnahmen erfordern eine gesonderte Genehmigung.
- Daten aller Art, die im Rahmen der Abarbeitung des Auftrags für die GASAG-Konzerngesellschaften generiert werden, befinden sich im Eigentum der beauftragenden GASAG-Konzerngesellschaft.
- Nach Abschluss der Arbeiten sind Daten aller Art an die beauftragende GASAG-Konzerngesellschaft zurückzugeben, wobei keine Kopien, Auszüge oder sonstige vollständige oder teilweise Reproduktionen einbehalten werden dürfen.

4 Hard- und Software

- Die Nutzung von Hard- und Software im GASAG-Netzwerk, die sich nicht im Eigentum der GASAG befindet oder durch die IT-Konzernstrategie genehmigt wurde, ist nicht zulässig.

  Die Installation von Hard- und Software, die sich nicht im Eigentum der GASAG befindet oder durch das Unternehmen genehmigt wurde, auf GASAG-Systemen ist nicht zulässig. Sämtliche Ausnahmen erfordern eine gesonderte Genehmigung.

- Die Anbindung von GASAG Ressourcen an fremde IT-Systeme oder -Dienste ist ohne ausdrückliche Genehmigung des Eigentümers nicht zulässig.

5 Regelungen zur Internetnutzung

- Wurde die Internetnutzung genehmigt, ist die Nutzung von Internetdiensten ausschließlich dann gestattet, wenn diese im Zusammenhang mit der Auftragserfüllung steht. Der Zugriff auf das Internet ist durch Inhalts-Filter eingeschränkt. Internetverbindungen werden anonym protokolliert.

6 Regelungen zur E-Mail-Nutzung

Zur Erleichterung der auftragsbezogenen Kommunikation können E-Mail Accounts innerhalb der GASAG Domain eingerichtet werden.

- Die Nutzung des internen E-Mail-Dienstes ist ausschließlich im Zusammenhang mit dem Auftrag gestattet. Die private Nutzung ist nicht gestattet.
- Die Versendung von E-Mail an externe Empfänger außerhalb der GASAG-Domäne ist nicht zulässig. Ausnahmen sind ausdrücklich zu genehmigen.
- Die automatische Weiterleitung von E-Mails an externe Postfächer ist nicht zulässig. Ein externer Zugriff auf das GASAG-Mail-Account kann per WebAccess nach Beantragung zur Verfügung gestellt werden.

7 Umgang mit Störungen und Problemen

- Bei Auftreten von Problemen im IT-Bereich wenden Sie sich bitte an Ihren Ansprechpartner des GASAG-Konzernunternehmens.
- Sicherheitsrelevante Ereignisse sind generell zu melden.
  Benachrichtigen Sie Ihren Ansprechpartner für technische Belange beispielsweise bei:
  - Datenverlust
  - Verlust ihres Passworts
  - Verlust von Hardware
  - Erkennung eines Virus auf Ihrem Rechner
  - Bemerken verdächtiger Aktivitäten.

8 Kontrolle von IT-Systemen

Die GASAG-Konzernunternehmen sind berechtigt, Handlungen im Rahmen von IT-Systemen, die an das GASAG-Datennetz angebunden sind, sowie an Benutzerkonten zurückzuverfolgen und zu protokollieren.

9 Bereitstellung von Fernzugriffen

Das nachstehende Kapitel nennt die Voraussetzungen und Rahmenbedingungen unter denen Fernzugriff auf die Systeme der GASAG-Gruppe gewährt wird.

9.1 Nutzungsbedingungen

Die Nutzung des Fernzugriffs ist nur zur Erbringung der Dienstleistung zulässig. Die im Fernzugriff verfügbaren Daten sind vertraulich zu behandeln. Der Fernzugriff wird personenbezogen gewährt und ist nicht übertragbar. Sämtliche Aktivitäten auf per Fernzugriff verfügbar gemachten Systemen können durch die GASAG-Konzernunternehmen protokolliert werden. Die per Fernzugriff verfügbar gemachten Ressourcen sind sorgsam und schonend zu behandeln. Bei nicht dedizierten Systemen gilt dies insbesondere in Hinblick auf die Systemperformance.

9.2 Zentrale Ansprechpartner

Der Dienstleister hat einen Mitarbeiter benannt, der für alle IT-Sicherheitsaspekte der Dienstleistungserbringung verantwortlich ist. Das beauftragende GASAG-Konzernunternehmen hat ebenfalls einen Ansprechpartner benannt (Anlage Verpflichtungserklärung).

9.3 Vertraulichkeit

Der Dienstleister verpflichtet sich und seine mit der Dienstleistungserbringung betrauten Mitarbeiter zur strikten Vertraulichkeit. Sämtliche Informationen über technische Konfigurationen, wirtschaftliche Lage, organisatorische Informationen, die mittels Fernzugriff bekannt werden, sind ausschließlich zur Erbringung der Dienstleistung zu verwenden. Die GASAG IT-Strategie ist bei Verstoßen gegen die Vertraulichkeitsvereinbarung sofort zu informieren.

Sofern personenbezogenen Informationen im Fernzugriff verfügbar gemacht werden, hat der Dienstleister diese Informationen gemäß den anwendbaren Rechtsvorschriften zu verarbeiten.

Beschäftigte des Dienstleisters, die an der Leistungserbringung für die GASAG-Konzernunternehmen beteiligt sind, sind auch nach Beendigung der Bereitstellung oder Ausscheiden des Betreffenden aus dem Beschäftigungsverhältnis mit dem Dienstleister zur Einhaltung der Datenschutzbestimmungen zu verpflichten.

9.4 Sicherheitsüberprüfung

Um die Sicherheit der GASAG Konzern-Systeme zu gewährleisten, werden Mindestanforderungen an die Absicherung der Clients und sonstigen Systeme des Dienstleisters gestellt. Diese Mindestanforderungen sind in Anhang 2 aufgeführt. Die GASAG IT-Strategie ist berechtigt, in Bezug auf die vom Dienstleister erbrachten Dienstleistungen technische Überprüfungen aller Sicherheitsaspekte durchzuführen. Dabei entdeckte Schwachstellen werden in zwei Kategorien zusammengefasst.

1. Verstöße
Verstöße gegen die Mindestanforderungen führen zur Sperrung des Fernzugriffs. Die unverzügliche Behebung durch den Dienstleister wird von der GASAG IT-Strategie erwartet. Der Fernzugriff wird nach erneuter Prüfung wieder gewährt.

2. Mängel
Bei kleineren Mängeln wird die Beseitigung durch den Dienstleister von der GASAG IT-Strategie erwartet. Die Entscheidung darüber liegt allerdings bei Dienstleister. Die Berechtigung zum Fernzugriff bleibt bestehen.

9.5 Verfügbarkeit

Die GASAG Konzernternehmen unternimmt im angemessenen Umfang Maßnahmen, um die Verfügbarkeit des Fernzugriffs, auf die zur Leistungserbringung notwendigen Systeme zu gewährleisten, garantiert jedoch keine ununterbrochene Verfügbarkeit.

Die GASAG IT-Strategie kann den Fernzugriff ohne Nennung von Gründen und ohne in Kenntnissetzung des Dienstleisters aussetzen, sofern die Sicherheit der GASAG-IT-Systeme gefährdet ist.

9.6 Haftung

Die GASAG-Konzernunternehmen übernehmen 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 den GASAG-Konzernunternehmen entstehen, haftbar. Eine solche Haftung schließt jedoch weder andere Ansprüche aus noch stellt sie eine Außerkraftsetzung der GASAG-Konzernunternehmen per Gesetz oder anderweitig zustehenden Rechte und Rechtsmittel dar.

9.7 Beginn / Beendigung

Der Fernzugriff wird bereitgestellt, sobald der Dienstleister einen hinreichenden Nachweis gemäß Anhang 2 erbracht hat, dass alle Bestimmungen dieser Richtlinie erfüllt sind. Soweit ein entsprechender Nachweis nicht erbracht werden kann, erfolgt keine Einrichtung des Fernzugriffes.

Die erteilten Fernzugriffe enden bei Auslaufen von Verträgen (Werk-, Dienstleistungs-, Supportverträge etc.).

Bei Beendigung der Vertragsverhältnisse gibt der Dienstleister innerhalb von 10 Werktagen alle Geräte zurück, die zur Ermöglichung des Fernzugriffs von GASAG-Konzernunternehmen bereitgestellt wurden.

9.8 Technische Spezifikation

Der Dienstleister erhält Fernzugriff in Form der in Anhang spezifizierten technischen Lösung. Änderungen der technischen Lösung stellen keine Änderung dieser Richtlinie dar. Zu Projektdokumentationszwecken sind die von der GASAG IT-Strategie vorgegebenen Standards einzuhalten.

9.9 Weitere Bestimmungen

Die vollständige oder teilweise Ungültigkeit von Punkten dieser Richtlinie beeinträchtigt nicht die Gültigkeit der anderen Punkte dieser Richtlinie. Änderungen der Richtlinie sowie ergänzende Bestimmungen, einschließlich der in diesem Punkt festgelegten Anforderung, bedürfen der Schriftform.

Anhang 1 Technische Spezifikation

1. Einrichtung des Fernzugriffs

Notwendige Arbeiten zur Einrichtung des Fernzugriffs auf die GASAG Systeme werden soweit es die GASAG-Konfiguration betrifft, vom jeweiligen IT-Dienstleister der GASAG durchgeführt. Der Dienstleister verpflichtet sich zur Kooperation mit diesem. Notwendige Arbeiten auf seiner Seite, gehen zu Lasten des Dienstleisters.

2. Varianten des Fernzugriffs

Nachfolgend werden Varianten des Fernzugriffs beschrieben. Die technische Detailbeschreibung kann auf Wunsch des Dienstleisters ausgehändigt werden. Die nachfolgend aufgeführte Variante 1 stellt den Standard zum Fernzugriff dar. Die Varianten 2 und 3 kommen nur zum Einsatz sofern Variante 1 nicht praktikabel ist.

2.1 Fernzugriff Variante 1 Site to Site VPN

Diese Variante bietet den uneingeschränkten Zugriff für komplette Netzsegmente auf die GASAG Infrastruktur. Die betreffenden Netze werden auf IP Basis transparent gekoppelt. Die notwendigen Konfigurationsparameter werden dem Dienstleister von der GASAG bereitgestellt. Dieser übernimmt die notwendigen Einstellungen auf seiner Seite der Fernzugriffs-Infrastruktur. Freigaben auf den beteiligten Firewalls werden projektbezogen nach dem „Minimalprinzip“ konfiguriert.

2.2 Fernzugriff Variante 2 SSL VPN mit Softwarezertifikat

Diese Variante bietet die Möglichkeit die Freigabe auf die GASAG Infrastruktur gezielt für einzelne Fernzugriffs-Ressourcen aus dem Dienstleisternetzwerk zu gewähren. Zugriff für komplette Netzsegmente auf die GASAG Infrastruktur. Für die Authentifizierung werden Softwarezertifikate der GASAG-PKI verwendet. Diese Zertifikate werden postalisch oder per E-Mail in verschlüsselter Form an den externen Partner versendet. Auf den Fernzugriffs-Ressourcen des Dienstleisters wird die für den transparenten VPN Zugang erforderliche Software durch den Dienstleister selbst installiert. Die Software wird dem Dienstleister von der GASAG gestellt.

2.3 Fernzugriff Variante 2.1 SSL VPN mit „Hardwarezertifikat“

Diese Variante bietet die Möglichkeit die Freigabe auf die GASAG Infrastruktur gezielt für einzelne Fernzugriffs-Ressourcen aus dem Dienstleisternetzwerk zu gewähren. In dieser Variante werden die Zertifikate auf einer Chipkarte gespeichert. Zu der Installation der VPN Software ist ein Kartenlesegerät notwendig. Das Zertifikat auf der Chipkarte und das Kartenlesegerät werden von der GASAG gestellt.

Anhang 2 Sicherheitstechnische Mindestanforderungen

Die technischen Mindestanforderungen orientieren sich am IT Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik.

Anforderung 1 – Dokumentierte Sicherheits-Richtlinie des Unternehmens
Der Dienstleister verfügt über eine schriftlich niedergelegte Richtlinie zur IT-Sicherheit. Diese Richtlinie wird durch den Dienstleister regelmäßig auf Ihren Erfüllungsgrad hin geprüft.

Anforderung 2 – Verantwortlichkeiten in Bezug auf Sicherheit
Der Dienstleister weist für die Sicherheit von Support und Wartung, Fernzugriffs-Ressourcen und Fernzugriffs-Infrastruktur klar definierte Aufgaben und Verantwortlichkeiten gemäß den in diesem Dokument genannten Anforderungen und Kontrollmaßnahmen zu.

Anforderung 3 – Vertraulichkeit
Vor Beginn der Nutzung des Fernzugriffs hat der Dienstleister von allen Angestellten, die er zur Nutzung des Fernzugriffs autorisiert hat, eine schriftliche Vertraulichkeitserklärung einzuholen, in der sie sich verpflichten, jegliche Information der GASAG bezüglich des Fernzugriffs vertraulich zu behandeln.

Anforderung 4 – Netzwerktrennung
Der Dienstleister hat die Fernzugriffs-Ressourcen, die mit Systemen der GASAG verbunden sind von allen anderen Netzwerken zu trennen. Diese Trennung kann entweder durch eine vollständige physikalische oder durch eine logische Trennung Isolierung. Der Aufbau der Remote-Computing-Infrastruktur ist dokumentiert.

Anforderung 5 – Absicherung
Ungenutzte Ports der Remote-Computing-Ressourcen und der Remote-Computing-Infrastruktur sind deaktiviert.

Anforderung 6 – Sicherer Datenverkehr
Es findet kein unverschlüsselter Datenverkehr zwischen den GASAG Systemen und den Remote-Computing-Ressourcen statt. Unsichere Zugänge (z. B. TELNET) zur Remote-Computing-Infrastruktur sind deaktiviert.

Anforderung 7 – Systemsicherheit
Fernzugriffs-Ressourcen des Dienstleisters sind durch Anti-Virus-Software geschützt. Zusätzlich gibt es ein Verfahren zur Verwaltung der Patches für Fernzugriffs-Ressourcen.
Anti-Virus-Signaturen der Virenscanner sowie der Patch-Status werden mit einem Dokumentierten Verfahren regelmäßig aktualisiert.