INFORMATIONS SICHERHEIT

Sicherheitsrichtlinie Informationssicherheit und Datenschutz
für IT-Fremddienstleister

Herausgegeben von den
Informationssicherheitsbeauftragten
der MVV Gruppe

Inhaltsverzeichnis

Erster Abschnitt
Allgemeine Bestimmungen

§ 1 Einleitung

Die MVV Gruppe hat ihre Strategie in Bezug auf Informationsschutz in einer übergeordneten Informationssicherheitsleitlinie festgelegt. Diese soll die Erfüllung der unternehmensinternen Vorgaben an Informationssicherheit und der gesetzlichen Vorschriften sicherstellen.

Aus diesem Grunde haben die Informationssicherheitsbeauftragten der MVV Gruppe Anforderungen an und Vorgaben für die Zusammenarbeit mit IT-Dienstleistern (nachfolgend „**Auftragnehmern**“ genannt) in dieser „**Sicherheitsrichtlinie Informationssicherheit und Datenschutz für IT-Fremddienstleister“** beschrieben. Sie gilt für IT-Leistungen aller Art für Gesellschaften der MVV Gruppe (nachfolgend „**Auftraggeber**“ genannt).

§ 2 Sicherheitsrichtlinie

(1) Diese Sicherheitsrichtlinie ist für den Zugang und Zugriff auf IT-Systeme, Dienste, Daten und Anwendungen in Netzwerken der MVV Gruppe (nachfolgend „**MVV Gruppen-Netzwerk**“ genannt) verbindlich.

(2) Im Einzelfall können zusätzliche auftrags- oder systembezogene Sicherheitsrichtlinien ergänzt werden.

(3) Der Auftragnehmer sorgt innerhalb seines Unternehmens und bei seinen Subunternehmen für die Beachtung dieser Sicherheitsrichtlinie.

Zweiter Abschnitt
Technische Sicherheitsrichtlinien

§ 3 Zugangs- und Zugriffsrechte

(1) Zugangs- und Zugriffsrechte auf das MVV Gruppen-Netzwerk werden nach Notwendigkeit gewährt und begrenzt. Die Einrichtung von Zugangs- und Zugriffsrechten für das MVV Gruppen-Netzwerk erfolgt durch den Soluvia IT-Anwenderservice.

(2) Ist für einen Auftragnehmer oder seine Subunternehmen ein Zugang/Zugriff zum MVV Gruppen-Netzwerk eingerichtet, sind die nachfolgenden Regelungen zu beachten:

1. Jeder Mitarbeiter des Auftragnehmers muss sich mit seiner Benutzerkennung anmelden und sichere Kennwörter[1] verwenden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass Zugang und Zugriffe auf das MVV Gruppen-Netzwerk protokolliert werden. Der Auftraggeber informiert hierüber seine Mitarbeiter und Subunternehmen. Benutzerkennungen und Kennwörter dürfen nicht weitergegeben werden.

2. Der Auftraggeber ist verpflichtet, den Soluvia IT-Anwenderservice umgehend zu informieren, wenn ein Zugang/Zugriff auf das MVV Gruppen-Netzwerk nicht mehr erforderlich ist (z. B. Auftragsabschluss, Mitarbeiterwechsel, Kündigung oder sonstige Beendigung des Auftrags).

3. Bei Auftragsbeendigung müssen die Mitarbeiter des Auftragnehmers und seine Subunternehmen alle durch den Auftraggeber überlassenen Arbeitsmittel (z. B. Ausweise und/oder Chipkarten, Token) an den Auftraggeber zurückgeben.

§ 4 Administrationsrechte

(1) Werden zur Erfüllung des Auftrags durch den Auftragnehmer Administrationsrechte benötigt, können diese nach Serviceanfrage des Auftraggebers eingerichtet werden.

(2) Die Einrichtung, Änderung und Löschung von Administrationsrechten für das MVV Gruppen-Netzwerk erfolgt durch den Soluvia IT-Anwenderservice.

(3) Voraussetzung zur Vergabe von Administrationsrechten ist die verbindliche Kenntnisnahme der Administratoren-Verpflichtungserklärung und die Teilnahme an einer Schulung zum Themengebiet Administratoren.

(4) Administratoren planen, installieren, konfigurieren und pflegen die informationstechnische Infrastruktur. Sie sorgen im Rahmen ihrer Administratorenaufgaben und -rechte für

- eine sachgerechte Installation,
- einen störungsfreien Betrieb,
- eine angemessene Pflege der IT-Systeme und Anwendungen und
- Beachtung der Ziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) im Verantwortungsbereich.

(5) Der Auftragnehmer bzw. seine Mitarbeiter und Subunternehmer mit Administrationsrechten haben die folgenden Richtlinien einzuhalten:

1. Die zum Zweck der Erfüllung des Auftrags eingerichteten Administrationsrechte dürfen ausschließlich für den vorgesehenen Zweck verwendet werden. Eine Weitergabe und/oder die Übertragung der zur Erfüllung der Aufgaben persönlich zugeordneten Administrationsrechte sowie diesbezüglicher Benutzerkennungen und Passwörter sind untersagt.

2. Werden aus technischen oder organisatorischen Gründen weitergehende Berechtigungen, als für die Erfüllung des Auftrags erforderlich, eingerichtet, dürfen dennoch nur die Berechtigungen genutzt werden, die zur Erfüllung des Auftrags zwingend benötigt werden.

[1] Sicheres Kennwort: mindestens 8 Zeichen, Verwendung von Groß-/Kleinschreibung, Zahlen, Sonderzeichen

3. Der unberechtigte bzw. außerhalb des Auftrags liegende Zugang und Zugriff auf IT-Systeme, Dienste, Daten und Anwendungen ist untersagt. Ist es aus technischen Gründen erforderlich, dass auf Daten mit persönlich zugeordneten Laufwerken bzw. Speicherbereichen zugegriffen werden muss, so darf ein solcher Zugriff nur mit der Einwilligung des betroffenen Anwenders erfolgen.

4. Das Überwinden von Schutzmaßnahmen und Verschlüsselungsmechanismen ist untersagt.

5. Bei der Durchführung von Administrationsaufgaben muss auf eine strikte Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der IT-Systeme, Dienste, Daten und Anwendungen geachtet werden.

6. Der Zugriff auf persönliche Laufwerke und Speicherbereiche kann ohne weitere Zustimmung des jeweiligen Anwenders durch den Administrator erfolgen, insofern eine technische Notwendigkeit wie Datenwiederstellung oder eine Störung dies erfordert. Gibt der Anwender einen Auftrag zur Beseitigung einer Störung oder beauftragt eine Leistung, die den Zugriff unmittelbar notwendig macht, gilt der Auftrag als Zustimmung.

7. Eine Massenverarbeitung von Daten in Folge technischer Umstände, wie beispielsweise Umzüge von persönlichen Laufwerken, Gruppenlaufwerken oder Postfächern, kann ebenfalls ohne Zustimmung der betroffenen Anwender erfolgen.

6. Für Administratoren sind Stellvertreter zu benennen. Bei Abwesenheit eines Administrators muss einem Stellvertreter der Zugang/Zugriff ermöglicht werden.

Es ist möglich, einem Stellvertreter im Vorfeld ein Passwort mitzuteilen, damit er bei einer Stellvertretung sofort Zugang/Zutritt hat.

Sollte ein Passwort erst im Fall der konkreten Stellvertretung vergeben werden, sind die Passörter in geeigneter Weise sicher zu hinterlegen (z.B. im Sekretariat in einem Safe in einem geschlossenen Umschlag). Es darf nicht möglich sein, dass Unbefugte auf die hinterlegten Passwörter Zugriff nehmen. Wird es notwendig, eines der hinterlegten Passwörter zu nutzen, so muss dies nach dem Vier-Augen-Prinzip, d.h. von zwei Personen gleichzeitig geschehen. Jeder Zugriff darauf muss dokumentiert werden. Nach Nutzung eines hinterlegten Passwortes muss durch den Administrator eine Aktualisierung des Passwortes stattfinden.

7. Werden auf Grund von personellen, organisatorischen oder technischen Maßnahmen oder Änderungen die Voraussetzungen der Administrationsrechtevergabe in Teilen oder gänzlich nicht mehr erfüllt oder werden Administrationsrechte nicht mehr benötigt, hat dies der Auftragnehmer unverzüglich dem Auftraggeber mitzuteilen.

§ 5 Schutz des Informationsverkehrs

Werden zur Erfüllung des Auftrags Informationen auf IT-Systemen des Auftragnehmers oder seiner Subunternehmen - außerhalb des MVV Gruppen-Netzwerk oder in dieses integriert – übertragen und/oder verarbeitet und ggf. mit dem Auftraggeber und/oder Unternehmen der MVV Gruppe ausgetauscht, sind zum Schutz der Informationen und des MVV Gruppen-Netzwerk nachfolgende Schutzmaßnahmen zu beachten:

(1) Der Auftragnehmer muss sicherstellen, dass auf der von ihm oder seiner Subunternehmen verwendeten und bereitgestellten Hardware (z. B. PCs, Server, Gateways) die aktuellste Version eines anerkannt sicheren Virenschutzsystems mit einer regelmäßig aktualisierten Virensignatur-Datenbank installiert ist, die Schutz gegen Angriffe durch Schadsoftware (z. B. Viren, Würmer, Trojanische Pferde) insbesondere via E-Mail, Web, mobile Datenträger (z. B. USB-Stick) oder anderen Medien bietet, indem sie den Dateizugriff kontrolliert.

(2) Werden vertrauliche Informationen zwischen dem MVV Gruppen-Netzwerk und dem Netzwerk des Auftragnehmers oder seiner Subunternehmen ausgetauscht, sind die Informationen nach Stand der Technik zu schützen und/oder muss die Übertragung/Transport über eine sichere Verbindung/Transportweg stattfinden. Für den Austausch streng vertraulicher Informationen ist eine Inhaltsverschlüsselung (Container, Hardwareverschlüsselung) und geschützte Übertragung/Transport Pflicht.

§ 6 Betriebssicherheit von IT-Systemen

(1) In Liegenschaften der MVV Energie zu nutzendes und insbesondere in das MVV Gruppen-Netzwerk zu integrierendes IT-Equipment des Auftragnehmers und/oder seiner Subunternehmen muss - sofern durch Soluvia IT freigegeben - zur Gewährleistung der Betriebssicherheit allen elektrischen und mechanischen Standards und dem Stand der Technik entsprechen.

(2) Für die Erfüllung des Auftrags erforderliche fremde Anwendungen und Software-Tools müssen vor ihrer Verwendung innerhalb des MVV Gruppen-Netzwerk durch den Auftraggeber genehmigt werden.

(3) Der Auftragnehmer und seine Subunternehmen müssen über einen definierten Patch-Management-Prozess sicherstellen, dass auf der von ihm verwendeten Hardware korrekt lizenzierte Software und regelmäßig aktualisierten Sicherheits-Patches für die Betriebssystem-Software und Anwendungen installiert sind.

§ 7 Integration von IT-Systemen

Werden einzelne Client- oder Server-Systeme oder Subnetze vom Auftragnehmer oder seinen Subunternehmen in das MVV Gruppen-Netzwerk integriert, sind nachfolgende Regelungen zu beachten, um eine wirksame Netzwerkzugangs/-zugriffskontrolle zu gewährleisten:

(1) Die Anbindung von Client-PCs eines Auftragnehmers oder seiner Subunternehmen in das MVV Gruppen-Netzwerk muss über einen Remote-Zugang für Externe erfolgen (dazu § 9).

(2) Bestehen weitergehende Anforderungen an eine unmittelbare Integration von Systemen des Auftragnehmers oder seiner Subunternehmen (z. B. zur Unterstützung von Produktionsprozessen oder Administration von MVV Gruppen-Systemen) müssen entsprechende Systeme oder Subnetze über eine Firewall vom MVV Gruppen-Netzwerk getrennt werden.

(3) Die Konfiguration der entsprechenden Regelbasis muss den Anforderungen der MVV Gruppe entsprechen, um den unautorisierten Zugriff des Auftragnehmers oder seiner Subunternehmen auf Nicht-Ziel-Systeme der MVV Gruppe oder die unbefugte Verwendung von MVV Gruppen-Diensten zu verhindern.

§ 8 Verbindung zu IT-Systemen

Erfolgt eine Anbindung von IT-Systemen aus Netzen des Auftragnehmers an das MVV Gruppen-Netzwerk, sind nachfolgende Regelungen zu beachten:

(1) Wenn zum MVV Gruppen-Netzwerk Verbindungen hergestellt werden, müssen der Auftragnehmer und seine Subunternehmen sicherstellen, dass ihr eigenes Netzwerk keinen unkontrollierten Zugriff durch Dritte auf das MVV Gruppen-Netzwerk ermöglicht. Jegliche Erstimplementierungen sowie sämtliche Änderungen der Netzwerkkonfiguration (Hardware/Software) mit Auswirkung auf die Sicherheit der Anbindung an das MVV Gruppen-Netzwerk müssen vorher mit dem Auftraggeber und/oder Soluvia IT abgestimmt werden.

(2) Der Auftraggeber übernimmt keine Verantwortung für etwaige Schäden an angrenzenden Systemen des Auftragnehmers oder seiner Subunternehmen, die auftreten können, während der Auftragnehmer oder seine Subunternehmen mit dem MVV Gruppen-Netzwerk verbunden sind.

§ 9 Remote Access Anbindung

(1) Eine Remote Access Anbindung ist vom Auftraggeber beim Soluvia IT-Anwenderservice zu beantragen.

(2) Vor Einrichtung eines Remote Access Zugangs erhalten Mitarbeiter des Auftragnehmers und seiner Subunternehmen zusätzlich zum Remote Access Antrag die „Sicherheitsrichtlinie Informationssicherheit und Datenschutz für IT-Fremddienstleister“ und eine „Verpflichtungserklärung auf das Datengeheimnis und die Informationssicherheit“. Der Remote Access Zugang wird für externe Mitarbeiter auf den Zeitraum der geplanten Dauer des Auftrags, höchsten aber auf sechs (6) Monate befristet.

(3) Es erfolgt eine Protokollierung und ggf. Auswertung der Aktivitäten. Der Auftraggeber informiert hierüber seine Mitarbeiter und Subunternehmen.

§ 10 Verwendung von Wireless-Komponenten

Bei Verwendung von Wireless-Komponenten des Auftragnehmers oder seiner Subunternehmen in Liegenschaften der MVV Gruppe dürfen bestehende Betriebseinrichtungen nicht beeinträchtigt werden und keine Verbindung zu dem MVV Gruppen-Netzwerk hergestellt werden.

§ 11 Sicherer System- und Anwendungsbetrieb

Werden IT-Systeme, Anwendungen und IT-Infrastrukturen im Auftrag des Auftraggebers durch den Auftragnehmer in Liegenschaften der MVV Gruppe oder des Auftragnehmers betrieben und/oder administriert (Anwendungs-Service-Provider), gelten die nachfolgenden Regelungen:

(1) Der Betrieb muss den Anforderungen des Informationsschutzes entsprechen, um als vertrauenswürdig anerkannt zu werden. Hierzu sind insbesondere

1. die gesetzliche Anforderungen einzuhalten,

2. die allgemeingültige Sicherheitsstandards nach BSI und/oder ISO 27001 zu beachten,

3. der Stand der Technik zur sicheren Erhebung, Verarbeitung, Speicherung und Aufbewahrung, Weitergabe sowie Löschung/Entsorgung schutzwürdiger Informationen und

4. die Anforderungen an Kommunikations- und Eskalationsprozesse bezogen auf Informationsschutzrelevante Ereignisse zu beachten.

(2) Der Auftragnehmer muss angemessene Vorsichtsmaßnahmen treffen, um die Hardware-Komponenten vor physischen Schäden zu schützen und die Verwendung durch unbefugte Benutzer zu verhindern.

(3) Der Auftragnehmer und seine subunternehmen müssen die Sicherheit der Betriebsumgebung gewährleisten sowie logische Zugangs- und Zugriffskontrollen implementieren, um eine effektive Trennung von Subnetzen zu gewährleisten.

(4) Beinhaltet der Auftrag die Erhebung, Nutzung oder Verarbeitung personenbezogener Daten im Sinne der Datenschutzgrundverordnung und des Bundesdatenschutzgesetzes, muss der Auftragnehmer alle aufgrund des Gesetzes erforderlichen Maßnahmen (Art. 32 DSGVO) zum Schutz der Daten treffen.

§ 12 Softwareentwicklung- und -integration

Erbringt der Auftragnehmer Leistungen der Softwareentwicklung und/oder -integration, sind unter Beachtung dieser Sicherheitsrichtlinie die projektspezifischen Sicherheitsanforderungen umzusetzen.

Dritter Abschnitt
Allgemeine Verpflichtungen

§ 13 Nutzung von Informationen des Auftraggebers

(1) Der Auftragnehmer und seine Subunternehmen sind verpflichtet, die vom Auftraggeber eingeräumten Zugangs-/Zugriffsrechte (IT-Systeme, Dienste, Daten und Anwendungen) ausschließlich im Rahmen ihrer vertraglich zu erfüllenden Verpflichtungen zu nutzen.

(2) Sämtliche durch den Auftrag erlangte, nicht öffentlich bekannte Informationen sowie auftragsbedingt erstellte Kopien, Aufzeichnungen und Arbeitsergebnisse sind Eigentum des Auftraggebers und an diesen nach Beendigung des Auftrages heraus- bzw. zurückzugeben.

(3) Der Auftragnehmer und seine Subunternehmen sind verpflichtet, alle ihm im Zusammenhang mit der Vertragserfüllung zur Kenntnis gelangten Informationen über den Arbeitgeber und Unternehmen der MVV Gruppe, ihre Geschäfts- und Betriebsangelegenheiten und alle Arbeitsergebnisse vertraulich zu behandeln und angemessen gegen eine Kenntnisnahme durch Unberechtigte und nicht vertragsgemäße Nutzung, Vervielfältigung oder Weitergabe zu schützen. Diese Verpflichtungen gelten über die Beendigung des Vertragsverhältnisses hinaus

(4) Dem Auftragnehmer und seinen Subunternehmen ist nicht gestattet, sich geschäftliche oder betriebliche, nicht von der MVV Gruppe öffentlich bekannt gemachte Informationen gleich welcher Art über Auftraggeber und/oder seine Kunden, Lieferanten oder Mitarbeiter anzueignen, für eigene Zwecke zu nutzen oder Kopien oder Aufzeichnungen irgendwelcher Art zu fertigen, soweit dies nicht zur Erfüllung des Auftrags erforderlich ist. Solche Informationen, Kopien, Aufzeichnungen oder Arbeitsergebnisse dürfen auch nicht an Dritte weitergegeben oder Dritten zur Kenntnis gebracht werden.

(5) Vertrauliche Informationen dürfen nur an die Subunternehmen weitergegeben werden, für die der Auftraggeber seine Zustimmung erteilt hat und die auf die Einhaltung der vorliegenden Sicherheitsrichtlinie verpflichtet wurden.

§ 14 Einhaltung der datenschutzrechtlichen Anforderungen und Geheimhaltungsverpflichtungen

Der Auftragnehmer darf beim Auftraggeber nur auf die Einhaltung datenschutzrechtlicher Anforderungen (DSGVO, BDSG), die Informationssicherheit und ggf. auf sonstige Geheimnisse (u. a. § 88 TKG) verpflichtetes Personal einsetzen. Die Verpflichtungen gelten auch nach Beendigung der Tätigkeit fort.

§ 15 Persönliche Eignung und fachliche Qualifikation der Mitarbeiter

(1) Der Auftragnehmer ist verpflichtet, ausschließlich Mitarbeiter beim Auftraggeber einzusetzen, die persönlich geeignet und fachlich qualifiziert sind. Die Beurteilung der Mitarbeiter ist vor Beginn des Auftragsverhältnisses durch den Auftragnehmer sicherzustellen. Dazu sollen unter anderem die folgenden Punkte geprüft werden:

- Verifikation der Person durch amtlichen Lichtbildausweis
- Verifikation des Lebenslaufs, der Qualifikationen und Arbeitszeugnisse
- Verifikation von akademischen Titeln und Abschlüssen
- Verifikation durch ein polizeiliches Führungszeugnis

(2) Es ist durch den Auftragnehmer sicherzustellen, dass Mitarbeiter, deren persönliche und/oder fachliche Eignung als nicht ausreichend bewertet werden können, weder Zutritt auf das Gelände oder in Gebäude noch Zugang zu den IT-Systemen des Auftraggebers erhalten.

(3) Auf Anfrage des Auftraggebers legt der Auftragnehmer dem Auftraggeber geeignete Unterlagen zur Überprüfung der persönlichen und fachlichen Eignung vor.

(4) Die Absätze 1 – 3 gelten entsprechend für Mitarbeiter von Nachunternehmen.

Vierter Abschnitt
Kontrolle der Einhaltung der Sicherheitsrichtlinien, Meldepflicht und Zugangs- und Zugriffsperrung

§ 16 Kontrolle der Einhaltung der Sicherheitsrichtlinien

(1) Der Auftraggeber hat das Recht, die Einhaltung dieser Sicherheitsrichtlinien auch am Standort des Auftragnehmers zu kontrollieren. Der Auftragnehmer hat dem Auftraggeber ferner die Kontrolle an den Standorten seiner Subunternehmer zu ermöglichen.

Der Auftragnehmer ermöglicht dem Auftraggeber insbesondere nach vorheriger Benachrichtigung und innerhalb der normalen Geschäftszeiten Zutritt zu allen relevanten Betriebsstandorten und unterstützt ihn bei allen erforderlichen Aktivitäten und Tests.

Er gewährt darüber hinaus Einsicht in für das MVV Gruppen-Netzwerk betriebsrelevante Dokumentation.

(2) Des Weiteren behält sich der Auftraggeber das Recht vor, die Art des Zugangs/Zutritts des Auftraggebers und/oder seiner Subunternehmen auf das MVV Gruppen-Netzwerk zu modifizieren, um die Sicherheit des MVV Gruppen-Netzwerks zu gewährleisten.

(3) Der Auftraggeber behält sich weiterhin das Recht vor, die IT-Infrastruktur des Auftragnehmers und seiner Subunternehmen, die mit dem MVV Gruppen-Netzwerk verbunden ist, in regelmäßigen Intervallen einer Risikoanalyse zu unterziehen und die Art des Zugriffs gemäß der aktuellen Sicherheitssituation zu ändern.

(4) Alle damit in Zusammenhang stehenden Kosten werden vom Auftragnehmer insoweit übernommen, als entsprechende Maßnahmen aufgrund von Änderungen der IT-Infrastruktur des Auftragnehmers oder seiner Subunternehmen erforderlich werden.

§ 17 Meldepflicht und Zugangs- und Zugriffssperrung

(1) Der Auftragnehmer ist verpflichtet, die für ihn einschlägigen Sicherheitsregelungen und Gesetze einzuhalten, sämtliche relevanten Fehler, Unregelmäßigkeiten oder Sicherheitsvorfälle sowie eingeleitete Maßnahmen zu deren Behebung im Zusammenhang mit dem MVV Gruppen-Netzwerk revisionssicher zu dokumentieren und dem Auftraggeber unverzüglich zu melden.

(2) Sollten diese Sicherheitsrichtlinien nicht eingehalten werden, behält sich der Auftraggeber das Recht vor, den Zugriff des Auftragnehmers und/oder seiner Subunternehmen auf das MVV Gruppen-Netzwerk sowie bestehende Anbindungen an das MVV Gruppen-Netzwerk ohne vorherige Ankündigung ganz oder teilweise zu sperren.

Dokumentensteuerung

Version	Stand	Bearbeitung durch	Bearbeitungsvermerk
1.0			
1.1	22.12.17	Weisbrodt	§ 11 Abs. 1 überarbeitet „erfüllen“ durch „beachten“ ersetzt
1.2	15.02.18	Weisbrodt	§ 15 komplett neu gefasst
2.0	30.07.18	Weisbrodt	Überarbeitung DSGVO