Merkblatt zur Informationssicherheit für externe Geschäftspartner der Unternehmen der Stadtwerke Stuttgart-Gruppe

1. Anwendungsbereich

Geschäftspartner der Unternehmen der Stadtwerke Stuttgart-Gruppe, die im Rahmen der Abwicklung eines Vertragsverhältnisses Zutritt zu Gebäuden oder Räumlichkeiten bzw. Zugang und/oder Zugriff auf elektronische Informationen bzw. Informationssysteme oder sonstige Informationen der Unternehmen der Stadtwerke Stuttgart-Gruppe erhalten, sind verpflichtet, die Regelungen dieses Merkblattes strikt einzuhalten, sofern keine anderen vertraglichen Regelungen vereinbart wurden.

Dieses Merkblatt gilt für alle Geschäftspartner, unabhängig davon, ob ihnen ein IT-Arbeitsplatz-System der Stadtwerke Stuttgart-Gruppe zur Verfügung gestellt wird oder sie mit ihren eigenen Systemen oder mit sonstigen Kommunikationstechnologien auf die Informationssysteme der Unternehmen der Stadtwerke Stuttgart-Gruppe zugreifen oder Informationen der Unternehmen der Stadtwerke Stuttgart-Gruppe verarbeiten.

2. Begriffsbestimmungen

Als Unternehmen der Stadtwerke Stuttgart-Gruppe gilt im Sinne dieses Merkblattes zur Informationssicherheit für externe Geschäftspartner jedes mit der Stadtwerke Stuttgart GmbH gem. §§ 15 ff. AktG verbundene Unternehmen. Verbundene Unternehmen in diesem Sinne sind insbesondere die Stuttgart Netze GmbH, die Stadtwerke Stuttgart Vertriebs GmbH oder die Energiedienste der Landeshauptstadt Stuttgart GmbH, sowie jede weitere rechtliche Einheit der Unternehmensgruppe der Stadtwerke Stuttgart GmbH, die von der Stadtwerke Stuttgart GmbH mittelbar oder unmittelbar kontrolliert wird.

3. Verantwortlichkeiten

Der Zutritt zu Lokationen und Räumlichkeiten der Unternehmen der Stadtwerke Stuttgart-Gruppe, der Zugriff auf Informationen der Unternehmen der Stadtwerke Stuttgart-Gruppe und/oder die Nutzung von Informations- und Kommunikationssystemen der Unternehmen der Stadtwerke Stuttgart-Gruppe erfordert vom Geschäftspartner und allen seinen Mitarbeitern und Unterauftragnehmern die strikte Einhaltung der in der Stadtwerke Stuttgart-Gruppe gültigen Sicherheitsvorgaben und Sicherungsmaßnahmen zum Schutz der Vertraulichkeit von Informationen, vor Bedrohungen durch Schadsoftware und Cyber-Angriffe und dergleichen. Die Verantwortung für die Einhaltung der Vorgaben liegt beim Geschäftspartner, auch für alle von ihm eingesetzten Unterauftragnehmer und deren Mitarbeiter. Dafür ist es zwingend erforderlich, insbesondere die nachfolgenden Regelungen einzuhalten. Die Unternehmen der Stadtwerke Stuttgart-Gruppe behalten sich vor, dem Geschäftspartner im Einzelfall weitergehende Weisungen zur Wahrung oder Wiederherstellung der Informationssicherheit zu erteilen.

4. Regelungen

1. Der Geschäftspartner muss die verbindliche Einhaltung aller Informationssicherheitsvorgaben arbeitsvertraglich für alle Mitarbeiter des Geschäftspartners geregelt haben.

2. Der Geschäftspartner muss seine Mitarbeiter regelmäßig in Bezug auf die Informationssicherheitsvorgaben und -anforderungen der Geschäftsbeziehung und aller zugehörigen Auftragsverhältnisse schulen und sensibilisieren.

3. Der Geschäftspartner muss für alle seine Mitarbeiter Vertraulichkeitsverpflichtungen geregelt haben. Dies muss so geregelt sein, dass die Verpflichtung, soweit rechtlich zulässig, über das Ende der betreffenden Geschäfts- bzw. Auftragsbeziehung und über das Ende des Beschäftigungsverhältnisses hinaus gültig bleibt.

4. Die Mitnahme von Dokumenten, Arbeitsergebnissen oder IT-Systemen außerhalb der Geschäftsräume und IT-Systeme der Unternehmen der Stadtwerke Stuttgart-Gruppe ist grundsätzlich nicht erlaubt und bedarf der vorherigen schriftlichen Genehmigung.

5. Der Zugang/Zugriff auf die IT-Systeme der Unternehmen der Stadtwerke Stuttgart-Gruppe darf nur über die jeweils zur Verfügung gestellten Endgeräte, Schnittstellen, Dienste und nur für die vereinbarten Zwecke und Aufgaben erfolgen.

6. Besondere Sicherheitseinstellungen, Sicherheitssysteme oder sonstige sicherheitsrelevante Vorkehrungen auf IT-Systemen der Unternehmen der Stadtwerke Stuttgart-Gruppe (z.B. zum Schutz vor Computerviren, Verschlüsselungen etc.) dürfen keinesfalls außer Betrieb genommen, umgangen oder in sonstiger Weise verändert werden.

7. Der Geschäftspartner hat bei Beendigung der Beauftragung alle vom beauftragenden Unternehmen der Stadtwerke Stuttgart-Gruppe erhaltenen Informationen und Unterlagen unverzüglich und unaufgefordert zurückzugeben und nach entsprechender Klärung mit und Bestätigung durch das beauftragende Unternehmen der Stadtwerke Stuttgart-Gruppe nicht zurückzugebende Informationen sicher zu vernichten, soweit diese nicht gesetzlichen Aufbewahrungspflichten unterliegen. Von den Unternehmen der Stadtwerke Stuttgart-Gruppe erhaltene Gegenstände, z.B. Zutritts-/Zugangskarten und -token, Schlüssel oder IT-Endgeräte, sind durch den Geschäftspartner unverzüglich zurückzugeben.

8. Der Geschäftspartner muss die durch die Unternehmen der Stadtwerke Stuttgart-Gruppe definierte Klassifizierung aller Informationen beachten und sicherstellen, dass die Informationen nach den für die jeweilige Klassifizierung geltenden Vorgaben der Unternehmen der Stadtwerke Stuttgart-Gruppe gehandhabt werden.

9. Der Geschäftspartner muss sicherstellen, dass nur diejenigen seiner Mitarbeiter Zugang zu Informationen der Unternehmen der Stadtwerke Stuttgart-Gruppe erhalten, die an der betreffenden Leistungserbringung beteiligt sind und die Informationen hierfür benötigen.

10. Die Authentifizierungsinformationen und -mechanismen (Kennungen, Passwörter, Hard- und Softwaretoken etc.) der Unternehmen der Stadtwerke Stuttgart-Gruppe dürfen ausschließlich strikt personenscharf verwendet werden. Eine Weitergabe an andere Personen oder Offenlegung gegenüber Dritten darf keinesfalls erfolgen. Gleiches gilt für jegliche Art von Ausweisen und Schlüsseln zur Zutrittssteuerung.

11. Wenn dem Geschäftspartner ein Fernzugang zu Systemen der Unterhemen der Stadtwerke Stuttgart-Gruppe gewährt wird, dürfen nur die vorgegebenen Gateways, Sprungserver und Dienste verwendet werden. Eine Netzkopplung oder parallele Fernzugriffe müssen strikt unterlassen werden.

12. Als Voraussetzung für die Einrichtung von Gast-Berechtigungen für Benutzerkennungen des Geschäftspartners bei Unternehmen der Stadtwerke Stuttgart-Gruppe muss der Geschäftspartner sicherstellen, dass mit seinen Benutzerkennungen ein Login ausschließlich über vom Geschäftspartner über Mobile Device Management verwaltete Endgeräte des Geschäftspartners möglich ist. Ein Login mit diesen Benutzerkennungen über jegliche anderen Endgeräte, z.B. private Endgeräte der betreffenden Mitarbeiter, muss zuverlässig unterbunden sein. Die Unternehmen der Stadtwerke Stuttgart-Gruppe behalten sich das Recht vor, Gast-Berechtigungen bei Zweifeln an der ordnungsgemäßen Nutzung zu verweigern oder jederzeit zu deaktivieren.

13. Der Geschäftspartner muss für seine eigenen Systeme, auf denen Informationen der Unternehmen der Stadtwerke Stuttgart-Gruppe verarbeitet werden, ein sicheres Authentifizierungsverfahren unter Nutzung starker Passwörter einsetzen und ausreichende Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware und Cyber-Bedrohungen einschließlich der dafür erforderlichen Schulung seiner Mitarbeiter sicherstellen.

14. Der Geschäftspartner hat sicherzustellen, dass ihm Informationen über mögliche Schwachstellen in von ihm verwendeten Systemen unverzüglich vorliegen und er daraufhin angemessene Maßnahmen zur Behebung und oder Risikominderung ergreifen wird.

15. Der Geschäftspartner muss die sichere Übertragung von Informationen und Daten über nach dem Stand der Technik verschlüsselte Übertragungswege sicherstellen.

16. Die Erbringung von Leistungen durch Unterauftragnehmer des Geschäftspartners darf nur im vertraglich vereinbarten Rahmen erfolgen. Sowohl die Nachvollziehbarkeit als auch das vom Geschäftspartner geforderte Sicherheitsniveau und die Einhaltung der vertraglichen Vereinbarungen mit den Unternehmen der Stadtwerke Stuttgart-Gruppe einschließlich dieses Merkblatts müssen durch den Geschäftspartner entlang der gesamten Leistungs- und Lieferkette sichergestellt sein.

17. Änderungen der Leistungs- und Lieferkette, Änderungen der Beteiligungsverhältnisse beim Geschäftspartner sowie geänderte Grundvoraussetzungen betreffend die Informationssicherheit, etwa die Aberkennung bestehender Zertifizierungen, sind vom Geschäftspartner unverzüglich an Stuttgart Netze GmbH zu melden.

18. Der Geschäftspartner muss das Management von Informationssicherheitsereignissen und -vorfällen gemäß den gesetzlichen Vorgaben und branchenüblichen Standards etabliert haben und damit effektive Reaktionen auf Informationssicherheitsereignisse und -vorfälle sicherstellen, die die Dienstleistung betreffen oder betreffen können. Dies umfasst auch einen zuverlässigen Meldeprozess des Geschäftspartners an das beauftragende Unternehmen der Stadtwerke Stuttgart-Gruppe für alle für die Geschäfts- und Auftragsbeziehung relevanten Ereignisse und Vorfälle.

19. Der Geschäftspartner muss das beauftragende Unternehmen der Stadtwerke Stuttgart-Gruppe unverzüglich über Schwachstellen, Ereignisse, Störungen und Vorfälle in Bezug auf die Informationssicherheit informieren, die einen Einfluss auf die Informationen der Stadtwerke Stuttgart-Gruppe und die Qualität der Dienstleistung haben könnten, und muss deren Handhabung mit dem beauftragenden Unternehmen der Stadtwerke Stuttgart-Gruppe abstimmen.

20. Der Geschäftspartner muss seine Mitarbeiter in Bezug auf die Erkennung, Meldung und Handhabung von Informationssicherheitsereignissen und -vorfällen laufend schulen und sensibilisieren.

21. Der Geschäftspartner muss die Unternehmen der Stadtwerke Stuttgart-Gruppe bei der Einhaltung der geltenden gesetzlichen, regulatorischen und vertraglichen Verpflichtungen und Anforderungen in Bezug auf die Informationssicherheit unterstützen.

22. Der Geschäftspartner muss insbesondere sämtliche einschlägigen gesetzlichen und regulatorischen Bestimmungen zur Informationssicherheit, zum Urheberrecht und zum Schutz personenbezogener Daten einhalten.

23. Das beauftragende Unternehmen der Stadtwerke Stuttgart-Gruppe ist berechtigt, eine regelmäßige Überprüfung der Einhaltung der Informationssicherheitsvorgaben im erforderlichen Umfang durchzuführen. Die Prüfung findet in Absprache mit dem Geschäftspartner statt und wird mit einer angemessenen Vorankündigungsfrist angemeldet. Dieses Audit-Recht schließt das Recht ein, jede Einrichtung des Geschäftspartners oder seiner Unterauftragnehmer, die Informationen der Stadtwerke Stuttgart-Gruppe verarbeiten oder beinhalten, zu besichtigen. Aufwände des Geschäftspartners im Zusammenhang mit solchen Überprüfungen werden nicht gesondert vergütet, sofern dazu keine anderslautende vertragliche Vereinbarung getroffen wurde.
    Der Geschäftspartner muss auch jeden seiner Unterauftragnehmer so verpflichten, dass die Überprüfung entsprechend ermöglicht wird.