STUTTGART

Landeshauptstadt Stuttgart Tiefbauamt mit Eigebetrieb Stadtentwässerung

Richtlinie Nr. 28

Lieferantenbedingungen - Informationssicherheit

Stand:	05.10.2024
Version:	1.20
Vertraulichkeit:	öffentlich

Daten und Informationen, die keinerlei Restriktionen unterliegen und abgesehen von urheberrechtlichen Aspekten ohne Einschränkungen weitergegeben oder veröffentlicht werden dürfen.

Versionsverwaltung

Datum	Autor	Version	Änderungen
20.01.2021	Benjamin Hecht	1.0	Initiale Erstellung
25.01.2021	Marc Breil	1.1	Ergänzung Umgang mit Schliessmedien
21.06.2022	Benjamin Hecht	1.11	Anpassen von 3.8.6
10.11.2022	Benjamin Hecht	1.12	Ergänzt um 3.5.6 & 3.5.7
29.11.2022	Benjamin Hecht	1.13	Thema polizeiliches Führungszeugnis angepasst
29.11.2022	Maik Szkudlarek	1.14	Unterschriftenfeld verstanden und bestätigt eingefügt
03.01.2023	Benjamin Hecht	1.15	Erweiterung um 3.11 – Konfiguration und Installation
20.3.2023	Marc Breil	1.16	Vertraulichkeit auf „öffentlich“ gesetzt (Einsatz bei Ausschreibungen)
24.04.2024	Benjamin Hecht Maik Szkudlarek	1.17	Inhaltliche Überarbeitung
20.06.2024	Benjamin Hecht Maik Szkudlarek	1.18	Sprachliche Anpassungen, eine Hierachieebene entfernt
04.07.2024	Benjamin Hecht	1.19	Rechtschreibfehler entfernt
05.10.2024	Benjamin Hecht	1.20	Abstimmung mit Rechtsamt

Inhaltsverzeichnis

1. Zweck des Dokuments ***4***
2. Begriffsdefinition ***4***
3. Allgemeines ***4***
4. Unteraufträge ***4***
5. Geheimhaltungsvereinbarung ***5***
5.1 Öffentlich 5
5.2 Nicht öffentlich 5
5.3 Intern 5
5.4 Vertraulich 5
5.5 Geheim 6
5.6 Nicht gekennzeichnete Informationen 6
5.7 Umgang mit klassifizierter Information 6
6. Personalsicherheit (HR-Security) ***8***
6.1 Vor der Beschäftigung 8
6.2 Während der Beschäftigung 9
6.3 Ende des Einsatzes beim Tiefbauamt 9
7. Umgang mit Werten (Assets) ***9***
7.1 Nutzung eigener und überlassener Werte 9
7.2 Sicheres Löschen 10
7.3 Wechseldatenträger 10
8. Regelung der Zugangsarten und Berechtigung ***10***
8.1 Zugangsregelungen 10
8.2 Zutritt und Umgang mit Zutrittsmedien 10
9. Umgang mit Vorfällen ***11***
9.1 Ereignisse und Vorfälle 11
9.2 Verschwiegenheit 11
10. Zuordnung von Rollen / kommunikations- und weisungsbefugte Personen ***12***

1. Zweck des Dokuments

Diese Richtlinie beschreibt, welche Informationssicherheitsanforderungen das Tiefbauamt der Landeshauptstadt Stuttgart mit Eigenbetrieb Stadtentwässerung (im weiteren Verlauf Auftraggeber (AG) genannt) an ihre Lieferanten/Dienstleister (im weiteren Verlauf Auftragnehmer (AN) genannt) stellen. Die Anforderungen ergänzen die allgemein gültigen Vertragsbedingungen des Tiefbauamtes um den Aspekt der Informationssicherheit.

2. Begriffsdefinition

Lieferanten: Unter den Begriff Lieferanten fallen alle externen Dienstleister, beispielsweise für Liefer-, Bau- und Dienstleistungen.

3. Allgemeines

Der Auftragnehmer (AN) hat die in der Industrie anerkannten Standards zu beachten und sein Verhalten eigenständig bei Änderung dieser Standards anzupassen.

Der AN hat dem AG die Kontaktinformationen seiner beim Amt eingesetzten Mitarbeitenden mitzuteilen.

Der AG wird entsprechend seine kommunikations- und weisungsbefugten Mitarbeitenden in einer Liste dokumentieren und an den AN kommunizieren. Arbeiten durch den AN sind ausschließlich gemäß Vertrag oder auf Weisung der in dieser Liste des AG erwähnten weisungsbefugten Personen auszuführen (s. Kapitel 10).

Sofern der AN nachweislich gegen eine Regelung dieser Richtlinie verstößt, so hat er einen Maßnahmenplan zur Umsetzung dieser Sicherheitsanforderung zu erstellen und nach Freigabe durch den AG umzusetzen.

Bei gravierenden Sicherheitsverstößen und -mängeln kann der AG die unverzügliche Beseitigung auf Kosten des AN fordern. Bei wiederholt unterlassener Mängelbeseitigung des AN behält sich der AG vor, eine Meldung an das BSI zu tätigen.

4. Unteraufträge

Der AN ist dafür verantwortlich, Sorge zu tragen, dass seine Lieferanten und Dienstleister alle Sicherheitsprinzipien aus dem Vertrag mit dem AG anwenden.

Der AN hat deshalb die hierin gestellten Sicherheitsanforderungen an alle im Rahmen der Erbringung der Dienstleistung beim AG eingesetzten Unterauftragnehmer über die gesamte Lieferkette für die zu erbringende Leistung durch vertragliche Vereinbarungen weiterzugeben. Der AN bleibt gegenüber dem AG, auch bei Einsatz von Unterauftragnehmern, allein verantwortlich für die Qualität der Dienstleistung.

Auf Verlangen des AG hat der AN die Weitergabe der hierin beschriebenen Anforderungen an seine Unterauftragnehmer nachzuweisen.

Vor Einsatz von Unterauftragnehmern hat der AN diesen von dem AG genehmigen zu lassen. Zu Dokumentationszwecken hat der AN eine Liste aller eingesetzten Unterauftragnehmer zu führen und diese dem AG zur Verfügung zu stellen.

5. Geheimhaltungsvereinbarung

Der AN verpflichtet sich und seine Mitarbeiter, alle im Rahmen des Vertragsverhältnisses erlangten vertraulichen Informationen, Geschäfts-und Betriebsgeheimnisse vertraulich zu behandeln. Ebenso verpflichtet sich der AN, alle Informationen hinsichtlich ihrer Vertraulichkeit zu klassifizieren, gut sichtbar zu kennzeichnen und entsprechend ihrer Klassifizierung zu schützen. Die Verpflichtung zur Wahrung der Vertraulichkeit gilt nach Ende des Vertragsverhältnisses sowie nach Ausscheiden der Mitarbeiter uneingeschränkt weiter.

Nachfolgend sind die zu verwendenden Klassifizierungsstufen definiert.

5.1 Öffentlich

Daten und Informationen, die keinerlei Restriktionen unterliegen und abgesehen von urheberrechtlichen Aspekten ohne Einschränkungen weitergegeben oder veröffentlicht werden dürfen.

Beispiele: Pressemitteilungen und Stellenausschreibungen

5.2 Nicht öffentlich

Die Daten und Informationen dürfen innerhalb des Tiefbauamts und an deren Partner frei weitergegeben, jedoch nicht veröffentlicht werden.

Beispiele: Vorgaben zum Arbeitsschutz, Arbeitsordnung, selbst entwickelte Schulungsunterlagen.

5.3 Intern

Informationen in dieser Stufe dürfen innerhalb des Tiefbauamts frei weitergegeben. Eine Weitergabe an externe Parteien ist ausschließlich im Rahmen der Erbringung von Dienstleistungen auf der Basis „Kenntnis nur wenn nötig“ erlaubt.

Konsequenzen beim Verlust der Vertraulichkeit sind denkbar, jedoch geringfügiger Natur (Schadenersatzansprüche einzelner Personen oder Organisationen sind z. B. wenig wahrscheinlich).

Beispiele: Dienstliche Kommunikationsdaten (z. B. Telefon-Nr., E-Mail-Adresse).

5.4 Vertraulich

Informationen in dieser Stufe dürfen an Empfänger innerhalb des Tiefbauamtes Stuttgart weitergegeben werden, jedoch nur auf der Basis „Kenntnis nur wenn nötig“. Eine Weitergabe an externe Parteien ist ausschließlich im Rahmen der Erbringung von Dienstleistungen und unter Verpflichtung zur Vertraulichkeit erlaubt. Der Informationseigner muss zusätzlich beabsichtigte

Einschränkungen der Weitergabe klar spezifizieren. Bei der Aufbewahrung muss sichergestellt sein, dass nur berechtigte Personen Zugang zu den Informationen besitzen.

Konsequenzen beim Verlust der Vertraulichkeit sind wahrscheinlich und messbar, z. B. Schadensersatzansprüche einzelner Personen oder Organisationen.

Beispiele: Personenbezogene Daten, die über dienstliche Kommunikationsdaten hinausgehen (z. B. Gehaltsdaten), Schaltpläne, Konfigurationsdateien.

5.5 Geheim

Informationen der Stufe „Geheim“ sind auf den Kreis der Anwesenden in einer Besprechung oder einer Video-/Telefon-Konferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist ohne Genehmigung des Informationseigners untersagt. In den meisten Fällen werden Informationen der Stufe „Geheim“ mündlich oder persönlich übergeben. Bei der persönlichen Informationsübergabe ist insbesondere auf einen geschlossenen Raum zu achten, so dass keine weiteren Personen Teile der Informationen erfassen können.

Eine Verletzung der Vertraulichkeit hat erhebliche Auswirkungen auf die Außenwirkung / das Erscheinungsbild des Tiefbauamtes und/oder wirtschaftliche Konsequenzen, z. B. massive Schadensersatzansprüche durch zahlreiche Personen oder Organisationen, Ausschluss aus bestimmten Märkten sowie nachteilige Auswirkungen auf das öffentliche Ansehen.

Beispiele: Besondere Arten personenbezogener Daten (z. B. Gesundheitsdaten),

5.6 Nicht gekennzeichnete Informationen

Ist eine Information nicht gekennzeichnet, ist diese implizit als "Intern" zu behandeln, es sei denn, es liegt eine Zustimmung der zuständigen Stellen zur Veröffentlichung vor. In diesem Fall sind die Daten und Informationen als öffentlich zu behandeln.

Liegt eine Ausnahmeregelung für einen Bereich und Informationstyp vor, so können nicht gekennzeichnete Informationen standardmäßig ebenso als vertraulich oder geheim gelten. Die Ausnahmegenehmigung wird bei Bedarf vom AG bereitgestellt. Der AN stellt sicher, dass alle mit den Informationen in Berührung kommenden Personen mindestens jährlich geschult.

5.7 Umgang mit klassifizierter Information

Die Regeln zum Umgang mit klassifizierten Informationen müssen von alle internen und externen Parteien befolgt werden.

	Öffentlich	**Nicht Öffentlich**	**Intern**	**Vertraulich**	**Geheim**
Dokumente	Uneinge-schränkte Weitergabe, außer urheber-rechtliche Beschränkung	Nur berechtigte Personen erhalten Zugang	Das Dokument darf sich nur in gesicherten Räumen befinden zu denen die Allgemeinheit keinen Zugang hat	Das Dokument muss in einem verschlossenen Schrank oder verschlüsselt aufbewahrt werden. Alternativ dürfen die Dokumente in einem	Das Dokument muss in einem Tresor oder digital verschlüsselt aufbewahrt werden.

	Öffentlich	Nicht Öffentlich	Intern	Vertraulich	Geheim
			Das Dokument muss regelmäßig von Druckern und Faxgeräten entfernt werden	Laufwerk abgelegt werden, auf das nur der berechtigte Personenkreis Zugriff hat. Das Dokument darf nur mithilfe der Funktion „privater Druck“ ausgedruckt werden. Das Dokument darf innerhalb der Organisation nur in versiegelten Mappen versendet werden.	Das Dokument darf innerhalb und außerhalb der Organisation nur durch eine vertrauenswürdige Person und in einem verschlossenen und versiegelten Umschlag übergeben werden. Digitale Dokumente müssen verschlüsselt übermittelt werden. Das Dokument darf nur mithilfe der Funktion „privater Druck“ ausgedruckt werden.
Informations-systeme	Uneingeschränkte Weitergabe, außer urheber-rechtliche Beschränkung	Nur berechtigte Personen dürfen Zugang erhalten	Der Zugang muss durch ein sicheres Passwort geschützt sein. Der Bildschirm muss automatisch nach spätestens 15 Minuten Inaktivität gesperrt werden. Das Informations-System darf sich ausschließlich in Räumen mit geschütztem physikalischen Zugang befinden.	Anwender müssen sich vom Informationssystem abmelden, falls sie sich vom Arbeitsplatz vorübergehend oder dauerhaft entfernen.	Das Informations-system darf ausschließlich auf Servern installiert werden, die unter der Leitung der Organisation stehen. Das Informations-System darf sich ausschließlich in Räumen befinden, bei denen die Identität von Personen vor dem Zutritt überprüft wird.
E-Mails	Uneingeschränkte Weitergabe, außer urheber-rechtlicher Beschränkungen	Nur berechtigte Personen dürfen Zugang erhalten	Der Absender muss die Empfänger-adresse sorgfältig prüfen.	Der Versand von E-Mails muss verschlüsselt erfolgen.	Der Versand von E-Mails muss verschlüsselt erfolgen.
Datenträger	Uneingeschränkte Weitergabe,	Nur berechtigte Personen dürfen Zugang erhalten	Datenträger oder Dateien müssen	Datenträger und Dateien müssen verschlüsselt sein.	Datenträger müssen in einem

	Öffentlich	Nicht Öffentlich	Intern	Vertraulich	Geheim
	außer urheber-rechtliche Beschränkung		passwortgeschützt sein. Der Datenträger darf nur in Räumen mit überwachtem physikalischem Zugang aufbewahrt werden.	Datenträger müssen in einem verschlossenen Schrank aufbewahrt werden.	Tresor aufbewahrt werden. Datenträger dürfen innerhalb und außerhalb der Organisation nur durch eine vertrauenswürdige Person und in einem verschlossenen Behältnis übergeben werden.
Mündlich weiter-gegebene Information	Uneingeschränkte Weitergabe, außer urheber-rechtliche Beschränkung	Nur berechtigte Personen dürfen Zugang zur Information erhalten Nicht berechtigte Personen dürfen sich nicht im selben Raum aufhalten, während die Information kommuniziert wird.	Die Zimmertüren sowie die Fenster müssen geschlossen sein. Es dürfen keine Telefonate zeitgleich im selben Raum geführt werden.	Die Unterredung darf nicht aufgezeichnet werden.	Besprechungen, die mit jeglicher Art von Kommunikations-mittel abgehalten werden, müssen verschlüsselt sein. Mitschriften der Gespräche sind nicht erlaubt.

*Die Maßnahmen verstehen sich kumulativ. Das heißt, Maßnahmen jeglicher Vertraulichkeitsstufe setzen die Umsetzung der Maßnahmen der niedrigeren Vertraulichkeitsstufen voraus. Falls strengere Maßnahmen für eine höhere Vertraulichkeitsstufe vorgeschrieben sind, werden nur diese umgesetzt.

6. Personalsicherheit (HR-Security)

6.1 Vor der Beschäftigung

Bereits vor dem Einsatz beim AG sind die möglichen Auswirkungen auf die Informationssicherheit durch das eingesetzte Personal zu berücksichtigen.

Die Angaben, Identität und der Hintergrund von den für Arbeiten beim AG eingesetzten Beschäftigten sind zu überprüfen. Die Überprüfung muss für alle Beschäftigte des AN durchgeführt werden, die Zugriff auf Systeme, Anlagen oder vertrauliche Informationen des AG erhalten.

Die Ergebnisse des Überprüfungsprozesses sind im Entscheidungsprozess, ob ein Beschäftigter beim AG eingesetzt wird zu berücksichtigen und gegen die Risiken abzuwägen.

6.2 Während der Beschäftigung

Der AN setzt in jedem Fall ausschließlich Personal mit geeignetem Fachwissen und entsprechenden Aus- und Weiterbildungen beim AG ein.

Der AN hat seine Mitarbeitenden jährlich in Bezug auf die Einhaltung der Informationssicherheit beim AG zu sensibilisieren und dies zu protokollieren. Die Inhalte müssen regelmäßig gemäß dem Stand der Technik aktualisiert werden.

6.3 Ende des Einsatzes beim Tiefbauamt

Der AN hat sicherzustellen, dass bei der Beendigung des Einsatzes des jeweiligen Beschäftigten des AN die Informationssicherheit gewahrt bleibt. Dazu muss der AN mindestens folgende Aktivitäten vornehmen:

- Deaktivieren/Sperren der Benutzerkonten
- Deaktivieren/Sperren von physischen Zugangsberechtigungen
- Rückgabe der Werte (bspw. Schlüssel)
-

Die Durchführung dieser Aktivitäten muss vom AN dokumentiert werden. Diese Dokumentation ist dem AG unverzüglich und unaufgefordert zu übermitteln.

7. Umgang mit Werten (Assets)

Werte (bzw. Assets) im Sinne der Lieferantenbedingungen sind jegliche Komponenten und Informationen, welche schützenswert sind oder ein Risiko für die Informationssicherheit darstellen können. Beispiele hierfür:

- IT-Hardware (Laptops, Server, Netzwerkkomponenten, Peripheriegeräte, Wechseldatenträger, …)
- Software (Anwendungssoftware, Betriebssysteme, Firmware, …)
- Dokumente (Papierdokumente, digitale Dokumente, …)

7.1 Nutzung eigener und überlassener Werte

Sofern es möglich ist, hat der AN Werte zu benutzen, welche ihm vom AG gestellt werden.

Werte des AN dürfen nur nach Zustimmung durch den Ansprechpartner des AG vorbehaltlich einer angemessen ausfallenden Risikoeinschätzung benutzt werden. Die hierbei eingesetzten Werte des AN müssen nach dem Stand der Technik geschützt sein.

Überlassene Werte müssen nach Ablauf des Vertragsverhältnisses oder auf Aufforderung durch einen berechtigten Verantwortlichen oder eine andere berechtigte Stelle des AG umgehend an den AG zurückgegeben werden.

Der AN hat sicherzustellen, dass bei ihm gespeicherte Daten des AG in seinem Besitz verbleiben, da er für diese (z. B. im Falle eines Datenverlustes) haftet.

7.2 Sicheres Löschen

Datenträger, auf denen der AN Informationen des AG verarbeitet, sind nach deren Einsatz vollständig durch Überschreiben zu löschen und physikalisch zu zerstören.

Der AN hat beim Löschen von Datenträgern den DoD-Löschstandard, den NIST-Löschstandard, oder ein gleichwertiges Verfahren zu nutzen.

Bei der Zerstörung der Datenträger sind die Anforderungen der DIN 66399 für Sicherheitsstufe 4 umzusetzen.

Für die Entsorgung von papierbasierten Informationen des AG hat der AN Schredder gemäß der in der DIN 66399 definierten Sicherheitsstufe 4 zu verwenden. Jeder Mitarbeitende des AN ist im Rahmen seiner Einarbeitung über die ordnungsgemäße Benutzung zu belehren.

Bei einer größeren Menge an zu entsorgendem Papier oder Datenträgern kann alternativ auch ein zertifizierter Entsorgungsdienstleiser herangezogen werden.

Als Nachweis für die sichere Entsorgung, Zerstörung oder Löschung muss ein Bericht erstellt und dem AG unverzüglich und unaufgefordert übermittelt werden.

7.3 Wechseldatenträger

Der AN darf nur durch den AG bzw. dessen Beauftragten bereitgestellte und freigegebene Wechseldatenträger mit Systemen des AG verbinden. Diese sind vor Anschluss an das System auf Schadsoftware zu untersuchen.

8. Regelung der Zugangsarten und Berechtigung

8.1 Zugangsregelungen

Der Zugang zu allen Systemen, Netzwerken, Diensten und Informationen ist für den AN grundsätzlich verboten, solange er nicht ausdrücklich erlaubt wird.

Sofern der AN für die Erbringung seiner Dienstleistung die Erstellung eines Kontos oder die Erteilung von Berechtigungen auf Informationssystemen des AG für seine Mitarbeitenden benötigt, hat er diese schriftlich beim AG zu beantragen.

8.2 Zutritt und Umgang mit Zutrittsmedien

Zutrittsmedien (Schlüssel, Zugangskarten, etc.) sind personenbezogen zu verwalten. Jegliche Weitergabe von Schlüsseln ist untersagt. Dies gilt auch für Personen innerhalb der eigenen Organisation. Die ausgegebenen Schlüssel sind ausschließlich für den autorisierten Gebrauch zu nutzen.

Schlüssel dürfen nicht gekennzeichnet werden so dass bei Verlust eine Zuordnung zur Funktion und den Räumen nicht ersichtlich ist.

Der Verlust eines Schlüssels ist umgehend dem Schlüsselwart zu melden.

Türen – insbesondere von Serverräumen – dürfen nicht offenstehen. Die Türen sind nach verlassen abzuschließen.

Unberechtigten Personen darf kein Zutritt gewährt werden.

9. Umgang mit Vorfällen

9.1 Ereignisse und Vorfälle

Ein Informationssicherheitsereignis wird als eine mögliche Beeinträchtigung der Informationssicherheit oder das mögliche Versagen von getroffenen Maßnahmen verstanden. Ein oder mehrere Informationssicherheitsereignisse können zu einem Informationssicherheitsvorfall werden, wenn sie bestimmten Kriterien entsprechen und/oder eine Bedrohung für die Werte des AG bzw. den störungsfreien Betrieb der kritischen Dienstleistung darstellen. Die Bewertung von Ereignissen anhand dieser Kriterien obliegt dem AG.

Informationssicherheitsvorfälle können unter anderem folgende Szenarien umfassen:

- Das Eindringen in Netzwerke oder Systeme, oder der Verdacht darauf
- Viren- oder Schadcodebefall
- Nicht vorhergesehenes Verhalten oder Beeinträchtigung der Funktionsweise von Anwendungen oder Systemen
- Jeder Versuch des unautorisierten Zugriffs oder Zutritts, oder der Verdacht darauf
- Ausfall von Systemen und Diensten
- Ungewöhnliche Meldungen aus Überwachungssystemen
- Ungewöhnliche Änderungen an Dateien
- Verstöße gegen die erlassenen Richtlinien
- Verstöße gegen die Geheimhaltung
- Diebstahl, Verlust oder Zerstörung von Geräten, Daten oder Informationen
- Ausnutzen von Schwachstellen
- Ausspähen von Informationen

Das reine Auftreten eines Informationssicherheitsereignisses bedeutet nicht zwingend eine Gefahr für die Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit von Systemen oder Daten.

Der AN hat dem ISB-TBA oder dem jeweils zuständigen SISB des AG unverzüglich alle Ereignisse bzw. Vorfälle, die unter die oben genannte Definition fallen, zu melden und diesen bei der Dokumentation und Behebung des jeweiligen Ereignisses bzw. Vorfalles zu unterstützen.

9.2 Verschwiegenheit

Alle beteiligten Beschäftigten des AN sind zur strikten Verschwiegenheit über die ihnen im Zusammenhang mit Informationssicherheitsereignissen oder Informationssicherheitsvorfällen beim AG bekanntgewordenen Informationen verpflichtet.

10. Zuordnung von Rollen / kommunikations- und weisungsbefugte Personen

Die hier dargestellte Zuordnung der Personen stellt den Stand bei Vertragsunterzeichnung dar. Änderungen hiervon sind möglich.

Abkürzung	Bedeutung	Kontaktdaten
ISB-TBA	Informationssicherheits-beauftragte*r Tiefbauamt	benjamin.hecht@stuttgart.de 0711-216-89892
SISB	Sektor-Informationssicherheits-beauftragte*r	Abwasser: maik.szkudlarek@stuttgart.de 0711-216-33088 Verkehr: gabriel.ott@stuttgart.de 0711-216-82911

Ich erkläre hiermit, dass ich die Vorgaben vollständig verstanden habe und befolgen werde. Mir ist bewusst, dass ein Verstoß gegen diese Vorgaben eine Verletzung meiner Pflichten darstellt.

Name: _____

Firma: _____

Datum: _____

Unterschrift: _____