

Verpflichtungserklärung

zwischen der

Stadtwerke Wiesbaden Netz GmbH

Konradinallee 25

65189 Wiesbaden

und dem Auftragnehmer

zur Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit unter der Beachtung der Vorgaben für die Datensicherheit bei Arbeiten am SCADA Netzleitsystem und den daran angeschlossenen Komponenten, bzw. auch Lieferung dieser Komponenten.

Im Rahmen der vereinbarten Dienstleistungen sind folgende nachstehenden Regelungen einzuhalten:

- Es ist untersagt, Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten oder zu nutzen.
- Bestehende Vorschriften über den Umgang bzw. die Sicherung dieser Daten sind zu beachten.
- Zum Schutz dieser Daten ist im Rahmen der zugewiesenen Aufgabe die notwendige Sorgfalt anzuwenden. Festgestellte Mängel sind dem ISB der *Stadtwerke Wiesbaden Netz GmbH* zu melden.
- Vertrauliche Informationen schriftlich, mündlich oder auf Datenträgern übermittelt, dürfen nur nach Zustimmung der sw netz an Dritte weitergegeben werden. Die Informationen sind dabei angemessen zu schützen. Die aktuelle Verschlüsselungsmethode ist beim Auftraggeber zu erfragen.
- Der Austausch der Daten erfolgt vorzugsweise über geschützte Filesharing-Plattformen.
- Beim Transport von Daten ist darauf zu achten, dass die Dokumente nur dem Adressatenkreis zur Einsicht gelangen dürfen. Sofern dies nicht möglich ist, ist die Form des Transports mit dem ISB abzustimmen.

- Beim Transport von Assets ist darauf zu achten, dass diese ebenfalls nur in Zugriff des Adressatenkreises gelangen dürfen, d.h. die Lieferkette muss in jedem Fall lückenlos nachvollziehbar sein.
- Lieferscheine sind mit dem deutlich sichtbaren Zusatz „Datensicherheitsrelevant“ zu versehen, damit die Gräte bei Anlieferung im Lager des Auftraggebers korrekt separat verschlossen werden können.
- Etablierte Zugangspasswörter der Assets dürfen nicht in der gleichen Hardwarelieferung zugesendet werden, diese sind vorzugsweise auch über Fileshare Plattformen zu kommunizieren.
- Erkennbare potentielle Schwachstellen, Abweichungen vom Verfahren oder erkennbare Gefahren sind dem Auftraggeber zu melden.

Die Verpflichtung auf das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort. Die Verpflichtungserklärung gilt auch für die Rechtsnachfolger der Parteien. Änderungen und Ergänzungen bedürfen der Schriftform.

Verstöße können strafrechtlich geahndet werden.

Neben der Beachtung der Vorschriften nach der DSGVO sind wir zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und zur Einhaltung der Grundsätze ordnungsgemäßer Datenverarbeitung verpflichtet. Daher werden alle Zugriffe auf die Kommunikationssysteme des Leitsystems protokolliert.

Es ist dafür zu sorgen, dass das eingesetzte IT- bzw. Telekommunikations-Equipment für den vorgesehenen Zweck zertifiziert ist, den einschlägigen Standards entspricht und angemessen geschützt ist. Die Arbeiten an den Assets dürfen nur nach dem Akzeptieren dieser Verpflichtungserklärung durch Fachpersonal durchgeführt werden.

Mit Annahme des Auftrags wird bestätigt, dass diese Verpflichtungserklärung verstanden und akzeptiert wird, sowie die Informationssicherheitsleitlinie_Extern berücksichtigt und eingehalten wird.