IT Sicherheitsrichtline

Für Dienstleistungen an IT-System der GfA und IT-System Lieferanten, im Folgenden als Auftragnehmer (AN) bezeichnet

(Stand: März 2023)

GfA Gemeinsames Kommunalunternehmen für Abfallwirtschaft Anstalt des öffentlichen Rechts der Landkreise Fürstenfeldbruck und Dachau

Josef-Kistler-Weg 22

82140 Olching

Tel.: 08142 / 2867-0

Fax: 08142 / 2867-92

Inhalt

1. Geltungsbereich und Zweck

Diese Sicherheitsrichtlinie ist verpflichtend für alle externen AN, die für die GfA tätig sind. Diese Vorgaben sind die Mindestanforderung für eine Leistungserbringung bei der GfA.

2. Verantwortlichkeiten

Der externe AN hat sicherzustellen, dass die Dienstleistungserbringung nach der hier vorliegenden Richtlinie erfolgt.

Der beauftragte externe AN hat jederzeit sicher zu stellen, dass sein Handeln und das Handeln seiner Beschäftigten nicht die Verfügbarkeit, Integrität oder Vertraulichkeit der IT-Systeme der GfA beeinträchtigt.

Urheberrechtliche und patentrechtliche Bestimmungen sowie Lizenzvereinbarungen sind einzuhalten.

Die bereitgestellten Zugangsdaten dürfen nicht ohne Genehmigung der GfA an Dritte weitergegeben werden.

3. Zugang zu Gebäuden und Produktionsstätten

Der externe AN muss seine Beschäftigten darauf hinweisen, dass diese sich vor Beginn der Arbeiten bei ihrem GfA-Ansprechpartner und der Warte anzumelden haben.

4. Nutzung von GfA IT-Systemen und IT-Infrastrukturen

a. Grundlagen

Die Nutzung der IT-Infrastruktur der GfA ist nur nach Freigabe durch den GfA Ansprechpartner gestattet. Eine Veränderung von Daten und Programmen, die nicht den vertraglich vereinbarten Leistungen entspricht, ist untersagt. Innerhalb der GfA Infrastruktur eingesetzte Hard- und Software darf die Sicherheit und Leistungsfähigkeit der Infrastruktur nicht beeinträchtigen. Die GfA behält sich vor, alle Zugriffe für Diagnose- und Sicherheitszwecke zu protokollieren.

Weiterhin muss der externe AN sicherstellen, dass seine Beschäftigten eine Unterweisung hinsichtlich IT-Sicherheit erhalten haben. Sollte zur Erbringung der Dienstleistung die Verarbeitung von personenbezogenen Daten notwendig sein bzw. wenn der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, muss der externe AN sicherstellen, dass seine Beschäftigten nach geltendem Datenschutzrecht unterwiesen und verpflichtet sind.

b. Nutzung von Internet und Kommunikationsinfrastruktur

Der externe AN hat seine Beschäftigten darauf hinzuweisen, falls der Zugriff auf Internetressourcen oder GfA-Kommunikationsplattformen bereitgestellt wurde, die Nutzung von Internet und Kommunikationsplattformen ausschließlich für geschäftliche Zwecke erlaubt sind.

IT-Systeme im Bereich Automatisierung und Steuerung dürfen keinen direkten Internetzugriff erhalten. Gleichzeitige Verbindung von IT-Systemen zu Automatisierungseinrichtungen/Steuerungen und Internet sind untersagt.

GfA - Josef-Kistler-Weg 22 - 82140 Olching - Tel: 08142 / 28 67-0 - Fax: 08142 / 16 54 1 - info@gfa-online.com - www.gfa-online.com

c. Nutzung von IT Systemen des externen AN

Das Verbinden von IT-Systemen des externen AN mit der IT-Infrastruktur der GfA ist grundsätzlich untersagt. Für Systemwartungen ist GfA-eigenes EDV-Equipment zu verwenden. Sollte es zur Verrichtung der Arbeiten notwendig sein, (z. B. aufgrund spezieller Software, die auf dem Notebook des externen AN installiert ist und zur Ausführung der Dienstleistung dringend erforderlich ist), das IT System an unseren Netzwerken (EDV / PLS / SPS) oder nicht vernetzten Rechnern anzuschließen oder direkt mit den Steuerungen (ABB-PLS / Siemens-SPS) zu verbinden, dann muss der AN dies vorab mit dem zuständigen GfA Ansprechpartner abstimmen, sowie nachweisen, dass auf dem IT System ein aktuelles Betriebssystem mit aktuellem Patchstand sowie ein aktiver Virenscanner mit aktuellem Stand der Viren-Datenbank installiert ist und ein Komplettscan zeitnah vorher durchgeführt wurde. Die GfA behält sich vor dies zu kontrollieren. Es darf nur ordnungsgemäß erworbene Software eingesetzt werden und der Softwareeinsatz muss mit dem zuständigen GfA Ansprechpartner abgestimmt werden.

d. Verwendung von externen Speichermedien/Datenträger/USB-Geräten

In der GfA IT Infrastruktur ist die Verwendung nicht zulässig. Über eine Datenschleuse können Dateien auf ein von der GfA zugelassenes Transfermedium kopiert werden.

e. Hard- und Softwaremanagement

Der externe AN darf nur IT-Komponenten bereitstellen, installieren oder verbauen, wenn diese vor ihrem Anschluss an das GfA-Netzwerk vom GfA-Ansprechpartner freigegeben worden sind.

Zur Freigabe der Hard- bzw. Software muss eine schriftliche Dokumentation mit folgenden Inhalten vorliegen.

- Übersicht Einbindung in die IT-Infrastruktur mit allen Schnittstellen.
- Geplante TCP/IP Adressbereiche/Subnetze.
- Eine detaillierte Beschreibung der gesamten Hardware.
- Eine Applikationsübersicht der eingesetzten Software inklusive Betriebssystem. Mindestangaben: Name, Hersteller, Version, Anzahl Lizenzen, End of Life Datum
- Freigabe Patches/Updates mit Patch/Updateplan
- Freigabe Virenscanner mit Freigabe Aktualisierung mit Patch/Updateplan

Gründe für Ausnahmen zu oben genannten Anforderungen müssen dem GfA Ansprechpartner erläutert werden und mit diesem abgestimmt werden.

Die vom externen AN eingesetzten IT-Komponenten müssen die von dem GfA gewählten IT-Sicherheitslösungen unterstützen. Der externe Dienstleister muss dies im Vorfeld mit der GfA abklären

Ausrangierte IT-Komponenten werden in Abstimmung mit dem GfA Ansprechpartner entsorgt.

5. Netzwerk

Jegliche nicht vom GfA-Ansprechpartner autorisierte Modifikation ist untersagt. Ein Netzwerkzugriff ist nur für vom GfA-Ansprechpartner freigegebene Endgeräte erlaubt. Die Verwendung und Betrieb von WLAN-Komponenten dürfen nur nach Freigabe durch den GfA-Ansprechpartner erfolgen. Ebenfalls ist der Betrieb von eigenen WLAN- sowie Bluetooth Netzwerken im Vorfeld mit dem GfA-Ansprechpartner abzustimmen.

6. Umgang mit Daten

Die Übertragung von Daten der GfA an Dritte ist nicht zulässig, sofern keine gesonderte Genehmigung vorliegt. Sämtlicher E-Mail-Verkehr zwischen der GfA und dem externen AN ist vertraulich zu behandeln. Das Speichern von **sensiblen** Daten der GfA in unverschlüsselter Form ist auf mobilen Datenträgern (z.B. USB-Sticks) unzulässig. Ausnahmen erfordern eine gesonderte Genehmigung durch den GfA-Ansprechpartner. Daten aller Art, die im Rahmen der Abarbeitung des Auftrags für die GfA generiert werden, befinden sich im Eigentum der GfA. Nach Abschluss der Arbeiten sind Daten aller Art an die GfA zurückzugeben, wobei keine Kopien, Auszüge oder sonstige vollständige oder teilweise Reproduktionen einbehalten werden dürfen. Ausnahmen erfordern eine gesonderte Genehmigung durch den GfA-Ansprechpartner.

7. Regelung bereitgestellte Benutzerkonten

Die erteilten Zugriffsberechtigungen und die Verwendung personenbezogener oder anderer betrieblichen Daten dienen ausschließlich der Erfüllung des Vertragsgegenstandes. Der externe AN hat dafür zu sorgen, dass sich jeder der eingesetzten Beschäftigten mit der für ihn beantragten Benutzerkennung anmelden kann. Die Benutzerkennung und das Passwort dürfen nicht an Dritte weitergegeben werden. Das Passwort muss den GfA Richtlinien entsprechen.

Bei Beendigung des Dienstleistungsvertrages muss der externe AN veranlassen, dass alle Ausweise und ausgehändigten Datenträger durch seine Beschäftigten an die GfA zurückgeben werden. Nicht mehr benötigte Benutzerkonten von Beschäftigten des externen AN müssen dem GfA Ansprechpartner zwecks Deaktivierung unverzüglich gemeldet werden. Weiter aktive Benutzerkonten des externen AN die auf dem IT System aus berechtigten Gründen verbleiben müssen, dürfen nicht mit einem „Standardpasswort“ geschützt werden.

8. Fernwartung / Fernzugriff

Der lokale Zugriff auf das GfA Netzwerk ist einem Fernzugriff immer vorzuziehen. Ein Fernzugriff ist nur in Abstimmung mit dem GfA Ansprechpartner und den nachfolgend aufgeführten Regelungen möglich.

Der Remote Zugriff zur Fernwartung wird nur über den mit dem GfA-Ansprechpartner eingerichteten Fernwartungszugang bereitgestellt, jegliche anderen Möglichkeiten werden nicht unterstützt / sind untersagt.

Der externe AN muss sicherstellen, dass das eigene Netzwerk seines Beschäftigten keinen unkontrollierten Zugriff Dritter auf das GfA Netzwerk ermöglicht. Kein IT-System darf eigenständig eine Verbindung nach extern aufbauen. Der externe AN ist verpflichtet, die Funktionalität des Fernzugriffs mindestens einmal nach Auftragsvergabe und anschließend einmal pro Jahr zu testen.

9. Umgang mit technischen Störungen

Der externe AN hat seine Beschäftigten darauf hinzuweisen, wenn während der Arbeiten Störungen auftreten oder ein IT-Sicherheitsvorfall bekannt/vermutet wird, dass umgehend der GfA-Ansprechpartner informiert werden muss.