

## Regelungen zur Nutzung von IT-Systemen für Externe

### 1. Zielsetzung

Sie haben von den Stadtwerken Dachau (nachfolgend SWD genannt) einen Geschäftsauftrag erhalten, für den Sie IT-Systeme der SWD nutzen werden. Um das Niveau der Informationssicherheit bei den SWD zu gewährleisten, wenn externe Dienstleistungen in Anspruch genommen werden, ist die Einhaltung bestimmter Regelungen nötig. Das vorliegende Dokument enthält die wichtigsten Verhaltensregeln für Anwender\*innen, damit unternehmenseigene Daten und Informationswerte geschützt werden. Die Einhaltung der nachfolgenden technischen und organisatorischen Sicherheitsmaßnahmen sind eine Grundvoraussetzung, um IT-Systeme der SWD nutzen zu dürfen.

### 2. Grundsätzliche Regelungen der Informationssicherheit

2.1 Die IT-Systeme und Anwendungen der SWD sind ausschließlich im Sinne der Ihnen zugewiesenen Aufgaben und Tätigkeiten zu nutzen. Es ist im SWD Kommunikations- und Prozessnetz untersagt, IT-Systeme zu nutzen, die nicht den SWD gehören. Sollte dies für die Auftragsabwicklung erforderlich sein, müssen Sie dafür eine Freigabe des zuständigen Systembetreibers bzw. Netzwerkbetreibers über den beauftragenden Fachbereich einholen.

2.2 Die Informationsressourcen der SWD müssen vor Schadsoftware geschützt werden.

a) Beinhaltet Ihr Geschäftsauftrag die Inbetriebnahme von Hard- und Software, müssen Sie diese vor der Installation auf Schadsoftware prüfen und die Freigabe des Systembetreibers bzw. des Anlagenverantwortlichen einholen.

b) Es ist verboten, Schadsoftware, Programme oder Hardware in den Kommunikations- und Prozessnetzen der SWD zu verwenden und/oder zu verbreiten, die Informationsressourcen verändern bzw. manipulieren können. Im Zuge von Sicherheitsaudits und Penetrationstests muss der Einsatz von Software zur Erkennung von Schwachstellen mit dem\*der Informationssicherheitsbeauftragten abgestimmt werden.

2.3 Personen- und unternehmensbezogene Daten dürfen nicht unbefugt an Dritte weitergegeben oder zu eigenen Zwecken verwendet werden. Sie dürfen diese Daten ausschließlich für die Erfüllung Ihres Auftrags nutzen.

2.4 Um die Sicherheit zu erhöhen, können Protokollierungs- und Auswertungsverfahren für Systeme und Anwendungen eingesetzt werden.

2.5 Vorfälle, die Auswirkungen auf die Informationssicherheit haben können (wie z. B. Anzeichen auf Virenbefall) müssen Sie unverzüglich dem Auftraggeber melden.

### 3. SWD Benutzerkennung

3.1 Für den Zugriff auf Informationsressourcen und Anwendungen erhalten Sie eine persönliche Benutzerkennung. Zugriffsberechtigungen und Passwörter dürfen nicht an Dritte weitergeben bzw. durch diese benutzt werden.

3.2 Im Rahmen eines Wartungs- und Bereitschaftsauftrages darf zur dynamischen Passwortgenerierung (Einmalpasswort) der ausgehändigte Token an berechnete und durch die SWD autorisierte Mitarbeiter\*innen weitergegeben werden.

3.3 Es ist untersagt, Benutzerkennungen anderer IT-Anwender\*innen auszuforschen und auszuprobieren.

### 4. Kommunikation

4.1 Falls keine Sonderregelung getroffen wurde, dürfen Sie Internet- und E-Mail-Dienste nur zur Erfüllung der beauftragten Tätigkeit verwenden. Die Dienste unterliegen zentralisierten und automatisierten Schutzverfahren (Virenabwehr, Spam-Prüfung, Blocken und Filtern von E-Mails, eingeschränkte Downloadberechtigungen und Webseiten-Sperlisten).

4.2 Verbindungen aus dem internen SWD Netzwerk zu Fremdnetzen (z. B. ins Internet) dürfen nur über dedizierte Firewall-Rechner erfolgen. Modems oder Funkverbindungen zu Fremdnetzen dürfen nicht in Kombination mit einer aktiven SWD Netzwerkanbindung verwendet werden.

4.3 Es ist untersagt, die Netztopologie oder die Konfiguration der IT-Systeme und -Anwendungen der SWD auszuforschen.

4.4 Einbindung von Fremdrechnersystemen

Wenn Fremdrechnersysteme auf Grund des Geschäftsauftrages eine Anbindung an die Netz- bzw. Domäneninfrastruktur der SWD benötigen, müssen folgende Bedingungen erfüllt sein:

- Aktueller und aktiver Virens Scanner (Engine und Pattern),
- aktueller Patchlevelstand für das Betriebssystem.

Bitte wenden Sie sich bei Fragen an Ihre fachlichen Ansprechpartner\*innen bei den SWD.

### 5. Fernwartung und Remotezugang zur IT-Infrastruktur der SWD

Remotezugänge und Netzkopplungen zur IT-Infrastruktur der SWD erfolgen nach festgelegten Regelungen:

5.1 Die Fernwartung erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen der SWD.

5.2 Der Auftragnehmer teilt den SWD vor Beginn der Fernwartung schriftlich mit, welche Mitarbeiter er dafür einsetzen wird.

5.3 Die Datenübertragungen hat nach Stand der Technik in verschlüsselter Form erfolgen.

5.4 Der Beginn jeder Fernwartung ist anzukündigen, um den Beauftragten der SWD die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen.

5.5 Der Verbindungsaufbau muss durch die SWD erfolgen bzw. durch die lokalen Systeme der SWD initiiert werden, so dass Wartungsarbeiten nur durch berechnete Personen und mit Wissen und Willen der SWD erfolgen.

5.6 Werden Daten (auch Programme, Updates, Patches) auf den Systemen der SWD gespeichert oder/ und gestartet, so ist mit geeigneten Mitteln sicherzustellen, dass diese frei von Schadsoftware sind.

5.7 Die SWD haben das Recht, die Fernwartung zu unterbrechen, insbesondere, wenn unbefugt auf Dateien oder auf nicht vereinbarte Hard- und Softwarekomponenten zugegriffen wird.

5.8 Der Zugang wird von den Systembetreibern der SWD protokolliert.

5.9 Abweichend von oben genannten Regelungen kann einem Externen, der im Auftrag der SWD Systeme in der Infrastruktur der SWD administriert bzw. wartet, ein Zugang gewährt werden, der nicht von Seiten der SWD initiiert werden muss. Dies bedingt, dass einer der folgenden Punkte zutrifft:

a) Aufrechterhaltung eines störungsfreien Betriebsablaufes

b) Gewährleistung einer zeitnahen Entstörung

c) Zugriff auf Test- / und Entwicklungssysteme

Davon unberührt bleibt die Pflicht zur Dokumentation, sowie die Meldung an die SWD zu Beginn des Fernzugriffs.

### 6. Überprüfung und Kontrolle

Der\*die Informationssicherheitsbeauftragte der SWD kann durch unangekündigte Kontrollen die Einhaltung der Vorgaben überprüfen.

### 7. Kenntnisnahme der Regelungen zur Informationssicherheit bei den SWD

Hiermit bestätige ich den Erhalt und die Kenntnisnahme des Dokuments:

## Regelungen zur Nutzung von IT-Systemen für Externe

---

Regelungen zur Nutzung von IT-Systemen  
für Externe

Firma: .....  
(Firmenstempel)

Name: .....

Vorname: .....

Datum: .....

Unterschrift: .....