Stadtwerke München

Informationssicherheit

Regelungen zur Nutzung von IT-Systemen für Externe

1. Zielsetzung

Sie haben von den SWM einen Geschäftsauftrag erhalten, für den Sie IT-Systeme der SWM nutzen werden. Um das Niveau der Informationssicherheit bei den SWM 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 SWM nutzen zu dürfen.

2. Grundsätzliche Regelungen der Informationssicherheit

2.1. Die IT-Systeme und Anwendungen der SWM sind **ausschließlich** im Sinne der Ihnen zugewiesenen Aufgaben und Tätigkeiten zu nutzen. Es ist im SWM Kommunikations- und Prozessnetz untersagt, IT-Systeme zu nutzen, die nicht den SWM 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 SWM 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 SWM 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 Informations-sicherheitsbeauftragten 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.

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

3. SWM Benutzerkennung

3.1. Der Zugriff auf Informationsressourcen, IT-Systeme und Anwendungen erfolgt über eine Mulit-Faktor-Authentisierung (MFA). Sie erhalten dazu eine persönliche Benutzerkennung und benötigen zusätzlich einen hard-/ oder softwarebasierten Mulit-Faktor. Der Software-Faktor (Token) wird über eine App auf

einem mobilen Endgerät des Auftragnehmers installiert. Die Zugangsinformationen (Benutzerkennung, Passwörter/ PIN) 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 berechtigte und durch die SWM 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-Sperrlisten).

4.2. Verbindungen aus dem internen SWM 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 SWM Netzwerkanbindung verwendet werden.

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

4.4. Einbindung von Fremdrechnersystemen

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

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

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

5. Fernwartung und Remotezugang zur IT-Infrastruktur der SWM

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

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

5.2. Der Auftragnehmer teilt den SWM 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 SWM die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen.

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

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

5.7. Die SWM 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 SWM protokolliert.

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

- Aufrechterhaltung eines störungsfreien Betriebsablaufes
- Gewährleistung einer zeitnahen Entstörung
- Zugriff auf Test- / und Entwicklungssysteme

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

6. Zutritt zu Räumlichkeiten der SWM

6.1. Verhalten in Geschäftsräumen der SWM

In Geschäftsräumen der SWM müssen folgende Verhaltensregeln eingehalten werden:

- Mitführen von SWM-Gastausweis bzw. Ausweisdokument der beauftragten Firma

- PCs, Laptops der SWM dürfen nicht ungefragt genutzt werden.
- Informationen und Medien, egal in welchem Format, dürfen nicht entwendet oder kopiert werden.
- Foto-, Video- und Ton-Aufnahmen sind untersagt.

6.2. Umgang mit Zutrittsmedien

Im Umgang mit Zutrittsmedien (Schlüssel, Ausweis) müssen folgende Regeln eingehalten werden:

- Zutrittsmedien dürfen niemals an andere Personen weitergegeben werden.
- Sie müssen sicher aufbewahrt werden.

Der Verlust eines Zutrittsmediums ist ein sicherheitsrelevantes Ereignis und muss durch den Beschäftigten umgehend gemeldet werden.

7. Überprüfung und Kontrolle

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

8. Kenntnisnahme der Regelungen zur Informationssicherheit bei den SWM

Hiermit bestätige ich den Erhalt und die Kenntnisnahme des Dokuments:

„REGELUNGEN ZUR NUTZUNG VON IT-SYSTEMEN FÜR EXTERNE“

Firma: ……

Name: ……

Vorname: ……

Datum: …… **Unterschrift: ……**