Besondere Bestimmungen Informationssicherheit bei Beschaffungen

Version 20. Juli 2022

1. Gegenstand und Geltung

Die vorliegende Beilage Informationssicherheit gilt bei IT-Beschaffungen von Hardware (HW), Software (SW), Dienstleistungen (DL) sowie bei Werkverträgen (WV).

2. Informationspflicht

2.1. Stellt die Leistungserbringerin fest, dass Systeme, die in Zusammenhang mit der Erbringung der Leistung stehen, kompromittiert sind oder möglicherweise kompromittiert sein könnten, hat sie unverzüglich die Leistungsempfängerin zu informieren.

2.2. Stellt die Leistungserbringerin fest, dass Daten der ETH Zürich offengelegt oder möglicherweise offengelegt sind, hat sie unverzüglich die Leistungsempfängerin zu informieren.

2.3. Stellen Mitarbeitende der Leistungserbringerin Unregelmässigkeiten fest, die auch negative Auswirkungen auf die IT-Systeme und Netze der Leistungsempfängerin haben könnten, muss die Leistungsempfängerin unverzüglich informiert werden.

2.4. Erhält die Leistungserbringerin Kenntnis von einer neuen Sicherheitsschwachstelle in den von ihr gelieferten Produkten, informiert sie ohne Verzug und allenfalls vor einer Veröffentlichung der Sicherheitsschwachstelle die Leistungsempfängerin und instruiert sie über mögliche, sofort anwendbare, mitigierende Massnahmen.

2.5. Unterlässt die Leistungserbringerin ihre Informationspflicht vorsätzlich oder fahrlässig, kann die Leistungsempfängerin Schadenersatz geltend machen.

3. Vertraulichkeit der Informationen

3.1. Vertrauliche Informationen der ETH Zürich dürfen nicht auf unverschlüsselten mobilen Endgeräten abgelegt oder mitgeführt werden.

3.2. Elektronisch übertragene Dateien mit vertraulichen Inhalten sind zu verschlüsseln. Geeignete Kommunikationskanäle werden zwischen der Leistungserbringerin und der Leistungsempfängerin vereinbart.

3.3. Elektronische Schlüssel sind streng vertraulich und entsprechend zu handhaben. Bei asymmetrischen Schlüsseln gilt: der private Teil dieser Schlüssel ist persönlich und darf nicht weitergegeben werden.

4. Integrität der Systeme

4.1. Es dürfen keine Anpassungen / Veränderungen / Manipulationen an Geräten und Einrichtungen der ETH Zürich vorgenommen werden, welche nicht durch den Auftrag der Leistungserbringerin abgedeckt sind.

4.2. Alle von der Leistungserbringerin auftragsgemäss gelieferten oder verwendeten Geräte und Programme müssen frei von bekannten Sicherheitsschwachstellen sein. Bei Geräten ist die Hardware inklusive Betriebssoftware und Firmware gemeint.

4.3. Erhält die Leistungserbringerin Kenntnis von einer neuen Sicherheitsschwachstelle in den von ihr gelieferten Produkten, liefert sie schnellstmöglich einen Fix für die entdeckte Sicherheitsschwachstelle. Diese Pflicht besteht auch nach der Lieferung weiter, solange die Produkte bei der Leistungsempfängerin unter Vertrag und im

Einsatz sind und die Leistungserbringerin die Produkte nicht schriftlich abgekündigt hat.

5. Fern- und Wartungszugriffe

5.1. Der Anschluss von IT-Systemen der Leistungserbringerin an die nicht öffentlich zugänglichen Netzwerke der Leistungsempfängerin mittels Kabel oder WLAN oder Fernzugriff bedarf in jedem einzelnen Fall einer schriftlichen Bewilligung der Leistungsempfängerin. Die anzuschliessenden Systeme müssen dauerhaft frei von bekannter Malware sein. Es dürfen keine Analysetools für Netzwerke und fremde Systeme oder Hackertools installiert sein.

5.2. Für bewilligte Wartungszugänge der Leistungserbringerin sind, wo immer möglich, Mehrfaktor-Authentifizierungen einzurichten und anzuwenden. Ist Mehrfaktor-Authentifizierung technisch oder aufwandsmässig nicht zumutbar, so müssen starke, persönliche Zugangspasswörter nach aktueller Best Practice verwendet werden. Diese Passwörter sind geheim zu halten.

5.3. Herstellerzugänge mit vorbelegten oder unveränderlichen (im Code hinterlegten) Passwörtern sind nicht erlaubt und müssen spätestens während der Installation der Systeme und Programme entfernt werden. Wird die Installation durch die Leistungsempfängerin selbst vorgenommen, muss die Leistungserbringerin sie auf das Vorhandensein solcher Herstellerzugänge hinweisen (Benutzerhandbuch).

5.4. Fernzugriffe auf das Netz der ETH Zürich aus öffentlichen Netzwerken oder Hotspots sind verboten. Sofern dafür die Notwendigkeit besteht, sind Fernzugriffe nur aus geschäftlichen, angemessen geschützten Netzwerken heraus erlaubt.

5.5. Sämtliche Zutritte zu nicht öffentlich zugänglichen Räumen der Leistungsempfängerin durch Personal der Leistungserbringerin erfolgen ausnahmslos begleitet.