Special provisions Information security in procurement

Version 20 July 2022

1. Subject matter and validity

This Information Security Supplement applies to IT procurements of hardware (HW), software (SW), services (DL) and contracts for work (WV).

2. Duty to inform

2.1. If the service provider discovers that systems related to the provision of the service are compromised or could potentially be compromised, it shall immediately inform the client.

2.2. If the service provider discovers that ETH Zurich data has been or may be disclosed, it must inform the client immediately.

2.3. If employees of the service provider detect irregularities that could also have negative effects on the IT systems and networks of the client, the client must be informed immediately.

2.4. If the service provider becomes aware of a new security vulnerability in the products it supplies, it shall inform the client without delay and, if necessary, before the security vulnerability is made public and instruct it on possible mitigating measures that can be applied immediately.

2.5. If the service provider intentionally or negligently fails to fulfil its duty to provide information, the client may claim damages.

3. Confidentiality of information

3.1. Confidential information of ETH Zurich may not be stored or carried on unencrypted mobile devices.

3.2. Electronically transmitted files with confidential content shall be encrypted. Suitable communication channels shall be agreed between the service provider and the client.

3.3. Electronic keys are strictly confidential and must be handled accordingly. In the case of asymmetric keys, the private part of these keys is personal and may not be passed on.

4. Integrity of the systems

4.1. No adaptations / modifications / manipulations may be made to ETH Zurich equipment and facilities that are not covered by the mandate of the service provider.

4.2. All devices and programmes supplied or used by the service provider in accordance with the contract must be free of known security vulnerabilities. In the case of devices, this means the hardware including operating software and firmware.

4.3. If the Service Provider becomes aware of a new security vulnerability in the Products delivered by it, it shall deliver a fix for the discovered security vulnerability as soon as possible. This obligation shall continue to exist after delivery for as long as the Products are under contract and in use by the client and the Service Provider has not discontinued the Products in writing.

5. Remote and maintenance access

5.1. The connection of IT systems of the service provider to the non-publicly accessible networks of the client by means of cable or WLAN or remote access requires the written consent of the client in each individual case. The systems to be con-

nected must be permanently free of known malware. No analysis tools for networks and third-party systems or hacker tools may be installed.

5.2. For authorised maintenance access by the service provider, multi-factor authentication must be set up and used wherever possible. If multi-factor authentication is not reasonable from a technical or cost point of view, strong personal access passwords must be used in accordance with current best practice. These passwords must be kept secret.

5.3. Manufacturer accesses with pre-assigned or unchangeable passwords (stored in the code) are not permitted and must be removed at the latest during the installation of the systems and programmes. If the installation is carried out by the client himself, the service provider must inform the client of the existence of such manufacturer accesses (user manual).

5.4. Remote access to the ETH Zurich network from public networks or hotspots is prohibited. If there is a need for this, remote accesses are only permitted from business, appropriately protected networks.

5.5. All access to non-publicly accessible rooms of the client by staff of the service provider shall be accompanied without exception.