TeamViewer

Overview of Technical and Organisational Measures

February 2022

Content

1 Access Control

1.1 Data Centers

TeamViewer does not own, lease or operate any TeamViewer server infrastructure for its offices or production environment. The TeamViewer production environment is a purely cloud-based infrastructure hosted in data centers provided by third parties.

TeamViewer has access control measures in place to prevent unauthorized access to data processing equipment where personal data is stored or processed.

1.2 TeamViewer Offices

Only authorized persons have physical access to premises, buildings or rooms where the personal data is processed. TeamViewer facilities are protected by key systems, intrusion detection systems, access control measures and active key management. Access rights are granted to authorized staff on an individual basis, including visitors who must be accompanied by authorized personnel. Employees and visitors are required to wear their badges visibly at all times when on the premises.

2 System Access and Access Control

TeamViewer relies on the following system access control measures to prevent unauthorized persons from using data processing systems where personal data is stored or processed.

2.1 Network and Hardware Security

The TeamViewer corporate network is protected from the public network by firewalls and threat detection as well as subsequent removal systems. The latest anti-virus/malware detection software is used to detect, remove and prevent malicious code. Security patch management is implemented and remote access to the TeamViewer corporate network is protected by strong authentication mechanisms and a Virtual Private Network (VPN).

TeamViewer uses a role-based security architecture and requires that users of the system be identified and authenticated before they can use system resources. Resources are protected by native security and add-on software products that identify and authenticate

users and validate access requests against users' authorized roles in access control lists. In situations where incompatible responsibilities cannot be separated, TeamViewer implements monitoring of one or more responsibilities. Monitoring must be performed by a supervisor without responsibility for performing the conflicting activities or by employees in a separate department.

All resources are managed in the asset inventory system and each resource is assigned an owner. The owners are responsible for approving access to the resource and performing checks on access by role.

Employees log in to the TeamViewer network with an Active Directory user ID and password. Users must also log in separately to any systems or applications that do not use Active Directory's split sign-on functionality. Passwords must meet defined password standards and are enforced by parameter settings in Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval. User IDs are locked after a certain number of unsuccessful login attempts to prevent access to system and resources. Additionally, after a defined period of inactivity, users' screens are locked automatically.

Employees accessing the system from outside the TeamViewer network must use a VPN tunnel and two-factor authentication system. Employees are issued VPN certificates when they are hired, and access is disabled when they leave.

TeamViewer employees access the two-factor authentication services over the Internet by using the Secure Socket Layer (SSL) functionality of their web browser. The employees first enter a valid user ID and password to gain access to TeamViewer cloud resources. The passwords must match the password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured according to TeamViewer configuration defaults, but these configuration parameters can be changed using the virtual server administration account.

TeamViewer maintains a System and Organization Control (SOC) that monitors critical systems and alerts around the clock to manage security incidents. These services are operated in a compliant and data protection-friendly manner while ensuring a threat response that is appropriate to the organization's risk level.

TeamViewer employees can log in to their systems via virtual server administration accounts. These administration accounts use a two-tier authentication system based on digital certificates.

User IDs and access rules are defined according to the role of each employee. Access rules are predefined based on the defined roles. When changes are made to a position, the associated rights and access rules are changed accordingly.

Annually, access rights are reviewed by team leaders and reconciled with the job description, tasks to be separated, and risks associated with access rights.

The revocation of rights and access as well as the deactivation of the account in the event of an employee's departure ("offboarding") or in the event of a change of position is carried out by the IT Service Desk to delete the employee's access or adjust the access rights.

Managers review the lists and enter the required changes into the event management record. The record is returned to the security help desk for processing. The IT Service Desk Manager identifies any records that have not been returned within two weeks and contacts the manager. As part of this process, the Information Security Officer (ISO) reviews employees with access to privileged roles and requests changes through the event management system.

Only authorized persons can access systems that process personal data. TeamViewer uses multiple authorization levels when granting access to systems. All employees access TeamViewer's corporate systems via a personalized account (user ID) and have access only to the systems they need to access to perform their duties. Authorizations and privileges are reviewed on a regular basis. Similarly, rights to access systems are reviewed when the employees are assigned new roles or leave TeamViewer.

TeamViewer has a password policy that governs the proper use and setup of passwords, including the frequency with which they must be changed, minimum requirements, and complexity.

2.2 Hiring ("Onboarding") and Departure ("Offboarding") of Employees

When an employee is hired, they are assigned to a position in the HR management system. 10 (ten) days before the employee's start date, the HR team creates a so-called "onboarding" ticket that contains the employee's user IDs and the access rights to be granted. The ticket is used by the IT service desk to create user IDs and access rules.

The access rules are defined according to the minimal principle (each employee is granted only the permissions he/she needs to perform his/her task). In addition, the ticket system contains a template for employees who change their position and the associated rights, which must be changed accordingly within the existing access rules.

Access rights are reviewed annually by team leaders to determine if they need to be revoked. When evaluating access rights, team leaders consider the job description, the tasks to be separated, and the risks associated with access rights.

After an employee's employment ends, the HR department again creates a ticket. These tickets are processed by the IT Service Desk to remove the employee's access in all systems. The IT Service Desk uses the tickets to lock user IDs and delete all access roles from IDs owned by the ticket's employee.

The lists of former employees are checked, and the desired changes are noted in the data record. The record is returned to the IT Security Help Desk for processing. The IT Service Desk Manager identifies any records that are not returned within two weeks and contacts the appropriate Team Leader. As part of this process, the Information Security Officer (ISO) reviews the employees with access to specific roles (including confidential roles) and implements changes through the system.

2.3 Data Access Control

TeamViewer controls access to systems containing personal data through a mixture of role-based access control (RBAC) and user rights management. This ensures that access to and use of data is minimized, both in terms of general processing and in terms of the list and scope of access for TeamViewer employees. These access controls vary depending on the sensitivity of the data stored and operational requirements.

2.4 Data Separation

The networks are segregated and segmented. This works within RBAC to minimize risks in line with sound security and data protection practices. For example, data for different products/purposes are processed separately where possible, including by separating production and test environments. Where appropriate, data is processed separately to avoid unnecessary mixing of data and processing beyond the purpose.

2.5 Pseudonymization

TeamViewer uses pseudonymization where it can be applied without affecting the efficiency of processes and/or where it is necessary to protect data in the event that disclosure is required. Where possible as part of the disclosure process, anonymization is used. Data that can identify data subjects contained in pseudonymized data is stored separately and encrypted where possible.

TeamViewer has a process for assessing internal data sharing and uses pseudonymization to limit the use of personal data for certain purposes.

3 Measures to Establish the Integrity

3.1 Transfer Control

TeamViewer has transfer controls in place to ensure that data is secure during transmission and that the level of protection does not fall below a minimum standard once it leaves the perimeter.

These security measures include securing transmissions with SSL/TLS, https, etc. and the use of VPNs throughout the organization. TeamViewer maintains firewalls and other standard security systems to protect its operations and data.

Firewall systems are in place to filter unauthorized incoming network traffic from the Internet and to deny any type of network connection that is not explicitly authorized. Network Address Translation (NAT) functionality is used to manage internal Internet Protocol (IP) addresses. Administrative access to the firewall is restricted to authorized personnel.

3.2 Data Input Control

TeamViewer has systems in place to log who has accessed or modified personal data, including linking such controls to individual accounts.

4 Data Availability and Resilience of the Systems

TeamViewer creates backups of critical data in accordance with common practice and ensures that these backups act as a reliable failover in the event of a catastrophic failure.

Customer data is backed up and monitored by Operations staff for completeness and disruptions. In the event of a disruption, the Operations staff performs troubleshooting to identify the root cause and then reruns the backup job immediately or as part of the next scheduled backup job, depending on the preferences specified by the customer in the documented work instructions.

Backup infrastructure is physically secured in locked cabinets and/or caged environments within third-party data center. The backup infrastructure resides on private networks that are logically secured from other networks.

Incident response policies and procedures are in place to guide the personnel in reporting and dealing with information technology incidents. Procedures are in place to detect, report, and respond to system security breaches and other incidents. Incident response procedures are in place to detect and respond to incidents on the network.

TeamViewer monitors the utilization of physical and computer infrastructure, both internally and for customers, to ensure that service delivery meets service level agreements.

TeamViewer evaluates the need for additional infrastructure capacity in response to the growth of existing customers or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following:

- Data centre space, power, and cooling
- Disk storage
- Tape storage
- Network bandwidth

TeamViewer has implemented a patch management process to ensure that the customer and infrastructure systems are patched in accordance with operating system patches recommended by the respective vendor. Customers and TeamViewer system owners review proposed operating system patches to determine if the patches are applied.

TeamViewer is responsible for determining the risk of applying or not applying patches based on the security and availability impact of these systems and any critical applications hosted on them. TeamViewer staff will verify that all patches have been applied and that a reboot has been performed, if applicable.

Redundancy is built into the system infrastructure that supports the data centre services to ensure that there is no single point of failure, which

includes firewalls, routers, and servers. If a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is performed to measure the security posture of a target system or environment. The commissioned third-party vendor uses an industry-standard penetration testing methodology specified by TeamViewer. The third-party vendor's approach begins with a vulnerability assessment of the target system to determine what vulnerabilities exist on the system that can be exploited through a penetration test, simulating a disgruntled/affected insider or an attacker who has gained internal access to the network.

Once the vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine if unauthorized access or other malicious activity is possible.

Penetration testing includes testing of the network and application layers, as well as testing of the controls and processes around the networks and applications. Testing is performed both externally (external testing) and within the network.

Vulnerability scans are performed weekly by TeamViewer in accordance with its internal policies. Upon request by a customer, a vulnerability scan may also be performed by a third-party vendor in accordance with TeamViewer policies. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by TeamViewer. These technologies are customized to efficiently test the organization's infrastructure and software while minimizing the potential risks associated with active scanning.

Retests and on-demand scans are performed as needed. Scans are performed outside of peak business hours.

Tools that need to be installed in the TeamViewer system are implemented via the change management process. Scanning is performed with approved scan templates and with bandwidth throttling options enabled.

Authorized employees can access the system over the Internet using VPN technology. Employees are authenticated by a token-based two-factor authentication system.

5 Data Protection Management

TeamViewer maintains a variety of privacy policies and procedures for which the Data Protection Officer (DPO) and TeamViewer management are ultimately responsible. TeamViewer continually updates its privacy and security measures in accordance with updated policies, applicable laws and

best practices. This includes regular reviews of documentation of procedures, training, and technical and organizational measures, maintaining and creating records of processing activities, and conducting data protection impact assessments as appropriate.

TeamViewer has processes, policies and procedures that describe physical security, logical access, computer operations, change control and data communication standards. All employees are obliged to adhere to TeamViewer policies and procedures that define how services are to be delivered. These are located on the company intranet and can be viewed by any TeamViewer employee.

The Employees receive regular data protection training and are bound to confidentiality. TeamViewer conducts regular awareness training for employees at least once a year, but the frequency may increase as needed.

TeamViewer designates at least one person per department who is responsible for compliance and implementation of the requirements of the General Data Protection Regulation (GDPR). All responsible data protection staff members have at least one IAPP CIPP qualification relevant to their area of work.

A review of the effectiveness of the technical and organizational measures is carried out at least annually. Data protection impact assessments are carried out when necessary.

There is a formalized policy for handling data subject requests under the GDPR.

All employees are trained internally in accordance with Art. 32 (4) GDPR and are obliged to ensure that personal data is handled in accordance with data protection requirements.

After termination of the contractual relationship, the data will be deleted in accordance with the principles of data protection with data minimization taken into account.

5.1 Subprocessors

TeamViewer enters into a Data Processing Agreements (DPA) with all subprocessors of personal data. Furthermore, TeamViewer ensures that all subprocessors comply with the relevant security and data protection standards and that these requirements and obligations are included as part of the DPA.

In the case of long-term cooperation, there is an ongoing review of the subprocessor and its level of protection.

5.2 Incident Response Management

TeamViewer has processes and tools in place to respond to security and other incidents, including firewalls, anti-malware systems, and collaboration between the DPO and the Chief Information Security Officer (CISO).

There is a documented process for detecting and reporting security incidents as well as data breaches (particularly with regard to the obligation to notify the supervisory authority) and a documented process for dealing with security incidents. Insofar as data processed on behalf is affected, a process ensures that the incident is immediately reported to the client, i.e., the controller as defined by the GDPR.

Security incidents and data breaches are documented and there is a formal process with assigned responsibilities for the follow-up and the implementation of any resulting actions.

6 Data Protection by Design and by Default

Personal data is collected and processed only to the extent necessary for the prescribed purpose. Data subjects have a simple way to exercise their rights.

Data protection principles are already observed during software development. In particular, the employees are encouraged and trained to implement technical and organizational measures as part of product development that ensure compliance with the requirements of GDPR and, specifically the rights of data subjects. The software is designed in such a way that the amount of data collected as well as the scope of processing is limited to the extent necessary. Insofar as various settings options exist within the software, the setting in which the smallest possible amount of personal data is processed is always selected in the delivery state.

With respect to change control, TeamViewer maintains documented Software Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include as follows: Change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is used to document change control procedures for changes in the application and implementation of new changes.

Quality assurance tests and results are documented and maintained along with the corresponding change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents these approvals in the ticketing system. Version control software is used to manage source code versions and migrate source code through the development process to the production environment. Version control software maintains a history of code changes to support rollback capabilities and tracks changes for developers.

All infrastructure changes to the environment are reviewed and approved by the Change Advisory Board (CAB). The CAB consists of, at a minimum, the Head of the IT Infrastructure, the Head of the Application and Demand Management, a member of the IT Security Team, and the change requestor. This ensures that all changes are reviewed, and that the quality of the implementation is maintained.

TeamViewer Germany GmbH
Bahnhofsplatz 2
73033 Göppingen
Germany

TeamViewer Germany GmbH
Bahnhofsplatz 2
73033 Göppingen
Germany