tresorit

Security Measures for Company Personal Data

19 October 2022

version: v4.0

Table of Contents

Version history

Version	Issue date	Status
v1.1	24 May 2018	Obsolete, revoked.
v2.6	22 October 2019	Obsolete, revoked.
v2.6.1	1 June 2020	Obsolete, revoked.
v3.0	21 March 2022	Issued, valid
v4.0	19 October 2022	Draft

1 INTRODUCTION

Tresorit is based on the principle that privacy is a fundamental human right of individuals. *Data security is not just a top priority for us, but it is our mission.* We invest significant resources in implementing the best solutions and practices to ensure the highest security level for our Customers' 'Company Personal Data' during our business relationship.

This document contains information about security measures that are implemented by Tresorit to comply with highest technical and organizational requirements. These controls also help to comply with Art. 32 of General Data Protection Regulation (GDPR).

1.1 Purpose & scope of document

This document provides an overview about the implemented security measures that are in place for our Customers' 'Company Personal Data' (all Personal Data provided to Tresorit by or on behalf of the Customer, through the Customers' or the Company Administered Users' use of services as defined in the Terms of Service).

Data types covered by this document are detailed in on our 'Privacy Policy' and Data Processing Agreement.

2 INFORMATION SECURITY MEASURES

In this chapter, we provide a detailed list about variety of security measures – based on confidentiality, integrity, availability and resilience of processing aspects – that we have implemented to ensure the highest security level for our Customers' 'Company Personal Data'.

Please note that our security practices are not limited to the mentioned ones, but – for security reasons – we haven't intended to disclose all applied safeguards.

2.1 Certification

Tresorit always pays attention to comply with applicable laws, as well as industry standard best practices to ensure the best security level of our Customers' 'Company Personal Data'.

As a demonstrable result of this intention, we have implemented actions based on ISO/IEC 27001:2013 'Information security management systems' standard. Tresorit has obtained this certification in May 2018 and keeps it valid by continuous work. Please find the details of our certification here:

https://www.certipedia.com/quality_marks/9108644476

2.2 Regulations

Tresorit has a comprehensive regulatory system in place covering the most important security, privacy, compliance and ethical rules. Internal regulations are published and communicated to all staff.

- It is mandatory for all employees to get familiar with them and for newcomers to sign a statement to accept rules.
- Our policies and procedures are reviewed at least yearly or in case of significant changes happened.

2.3 Organization

2.3.1 Screening

Background screening practice of Tresorit is always in line with legal regulations in force and ethics. Our method is also proportional to business requirements, classification of the information to be accessed and perceived risks. This background verification check is performed prior to allowing the person (employee, contractor or other third party) access any business resources.

2.3.2 Trainings

Tresorit thinks that training for employees is crucial to ensure better security level, therefore we take the following actions:

- Information security and privacy training is mandatory for newcomers.
- Mandatory information security and privacy training at least once a year to keep the staff's knowledge up to date.
- We also conduct casual training sessions and internal phishing tests based on the actual hot topics in security.

2.3.3 Security-related teams

- The Governance, Privacy, Risk Management & Compliance (GPRC) Team considers the information security and privacy aspects during the whole business process. This team is involved in projects to ensure relevant information security aspects and privacy are represented.
- The Legal Team considers the legal aspects during the whole business process. This team is involved in projects to ensure legal aspects are represented.
- The Security, Product & Engineering Enablement (SPEED) Team considers the cyber security and infrastructure security aspects during the whole business process. This team is involved in projects to ensure cyber security and infrastructure security aspects are represented.
- The engineering teams are made up of talented, highly educated members who are trained about the security aspects too.

2.3.4 Data Protection Officer

- Data Protection Officer (DPO) has been appointed by the Management.

- Where required, a data protection impact assessment (DPIA) is carried out prior to processing.
- We have a formal process in place to handle information requests.

2.4 Physical access control

The following physical access controls are applied to prevent unauthorized access, use, disclosure, or loss to our Customers' 'Company Personal Data'.
Based on our business model, we have outsourced the data storage for the data scope concerned. Please see the details of physical access control in Data Center chapter.

2.4.1 Office

For the purpose of building and area protection and as measures of access control, the following controls are implemented in our headquarter office building:

- Office building entry control:
  - Reception function with guard services (mandatory to sign into a visitor database).
  - Access control system (turnstiles) that works with RFID cards.
- Further control for Tresorit's office spaces entry:
  - Access control system implemented on those doors (works with the RFID cards).
  - Visitors must ring the doorbell, and the guest's RFID card is valid only for using the elevators.
  - We also have a Reception function in the office space (to welcome visitors).
- The office building itself is controlled by
  - Alarm system to detect unauthorized entry attempts.
  - Video surveillance system (CCTV system) to monitor the entrances (in the lift lobbies).

Tresorit also supports the physical access controls listed above with organizational measures:

- Based on our visitor policy, our guests are always accompanied by employees.
- We have an 'Event Security Policy' that implements extra security measures in case of any event held in our office space (e.g. to lock offices by physical keys during the event).

2.5 Logical access control

The following logical access controls are applied to prevent unauthorized access, use, disclosure, or loss to our Customers' 'Company Personal Data'.
Based on our business model, we have outsourced the data storage for the data scope concerned. Please see the details of logical access control in Data Center chapter.

2.5.1 Office

For the purpose of logical access control, the following controls are implemented in our headquarter office building (where our Customers' 'Company Personal Data' can be accessed):

- Tresorit's office network is controlled by
  - Malware protection solutions on client computers,
  - Firewall.
- Tresorit's devices are controlled by
  - Encryption of notebooks,
  - BIOS protection (separate password) on notebooks.
- Tresorit's user accounts' protection:
  - The login is possible by using unique username/ID and strong password. As alternate method login with biometric data is also possible (by fingerprint scanner on notebooks).
  - Useage of two factor authentication (2FA) on applications is mandatory, where it's available.
  - Automatic desktop lock and lockouts have been set for notebooks and PCs.

Tresorit also supports the logical access control detailed above with organizational measures:

- We have clear desk and clear screen policy in place, including instructions for mandatory manual user account locking when the user is leaving the workplace.
- Employees are enforced and also obliged to keep all pieces of security software up to date (e.g. malware-protection products) on their own devices. This is supported by automatic vulnerability scanner tool. Therefore, all devices are scanned regularly and we notify our colleagues.

2.5.2 Data management

2.5.2.1 Data access

To prevent unauthorized access, reading, copying, alteration or removal of our Customers' 'Company Personal Data', the following controls are implemented:

- User access right management procedures are in place based on 'need to know' principle. By this we make sure to only share the least possible amount of data needed to achieve essential business goals.
- Data of different Customers are stored logically separated from each other, and from our own data sets in the databases.
- We use pseudonymized data base for usage metrics we use for improving our service quality.
- We use a separate database and data set for testing purposes.
- As a digital company a small amount of paper document is used in our office. If it is necessary to print something containing confidential data, the paper will be stored securely or destroyed by document shredder after it became obsolete.

2.5.2.2 Data changes

Measures are in place to ensure that changes in data (entry, alteration and deletion) can be verified and determined are the followings:

- Essential system activities (as logins, logouts, edits to content, assignment of permissions, mails sent etc.) are logged.
    - Traceability of activity is possible by individual usernames (not user groups).

2.5.2.3 Data transfer

During a data transfer process (electronic transmission or their storage on data carrier media) the data are controlled by the following measures:

- No data carrier media is used for business operation.
- All data is encrypted during transit using advanced cryptographic protocols.

2.6 Risk assessment program

Tresorit has a documented, annually revised and audited information security risk assessment and risk management practice.

Defined asset – threat – control pairings are evaluated based on the predefined risk scale. Risks in unacceptable category are communicating to Management and they define actions to reduce these risks.

2.7 Incident management program

We assess information security and cyber security vulnerabilities with highest priority. Therefore, Tresorit has a documented, regularly revised and actualized security incident response plan. We also summarize lessons learned in case of any incident management event.

As a special type of incident, Tresorit has an implemented Data Breach Response and Reporting Procedure too.

We think that credibility is based on transparency, therefore incident history of our product is available on our homepage: https://status.tresorit.com/history.

2.8 Business continuity program

Critical business processes are defined by Tresorit's Board. As main function of our service is secure data storage, the most important of the critical business processes are 'Tresorit service maintenance' and 'Communication with existing customers'.

- Business Impact Analysis (BIA) are prepared for these critical processes.
- Business Continuity Plans (BCP) are prepared for these critical processes.
  - We train our staff for emergency situations and test BCPs regularly.
- Disaster Recovery Plans (DRP) are prepared for these critical processes.
  - We train our relevant staff members for emergency situations and test DRPs regularly.

2.9 Audits

2.9.1 Internal audit

We conduct internal audits regularly in information security and data protection topics (e.g. IT infrastructure settings, user access rights) to verify our security measures.

GPRC Team is responsible for tracking the implementation of correction actions for findings.

2.9.2 External audit

We use external auditors to verify the adequacy of our security measures.

- Tresorit has an ISO/IEC 27001:2013 certification audited annually by an auditor company member of internationally trusted TÜV Rheinland Group.

GPRC Team is responsible for tracking the implementation of correction actions for findings.

3 THIRD PARTIES

As any other business, we may need to use 3rd party service providers for billing, backup, analytics etc. We consider security and compliance as a top priority. Therefore, we always strive to choose security-conscious suppliers.

- We only work with highly respected suppliers having been in the business for years and holding a good track record of security aspects and business behavior.
- We apply an internal supplier security review procedure involved relevant colleagues. Suppliers are only approved if compliance with the technical and organizational measures are verified according to Art. 32 GDPR and ISO 27001 standard.
  For detailed list about our actual 3rd parties please see: https://support.tresorit.com/hc/en-us/articles/216114397-Third-party-services

3.1 Data Center

Based on our business model, we store our Customers' 'Company Personal Data' in the cloud. We have outsourced data storage activity to a market leading service provider, and we store our Customers' 'Company Personal Data' in Microsoft Azure Data Center.
Thus, measures designed and implemented for Tresorit's server rooms are not the scope of this document.

Microsoft Azure is implemented the best security techniques and has several security certificates granting the security of their infrastructure. For more information about Microsoft Azure Data Center's, please see the applied security measures on their official homepage (links of the security actions on the publishing date of this document):

- Physical security: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security
- Infrastructure security: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure
- Availability: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability
- Data protection: https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data

We rely on Microsoft Azure's Locally redundant storage (LRS) which is designed to attempt to reconstruct customer data in its original or last replicated state from before the time it was lost or destroyed.

- Azure Storage redundancy: https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy.