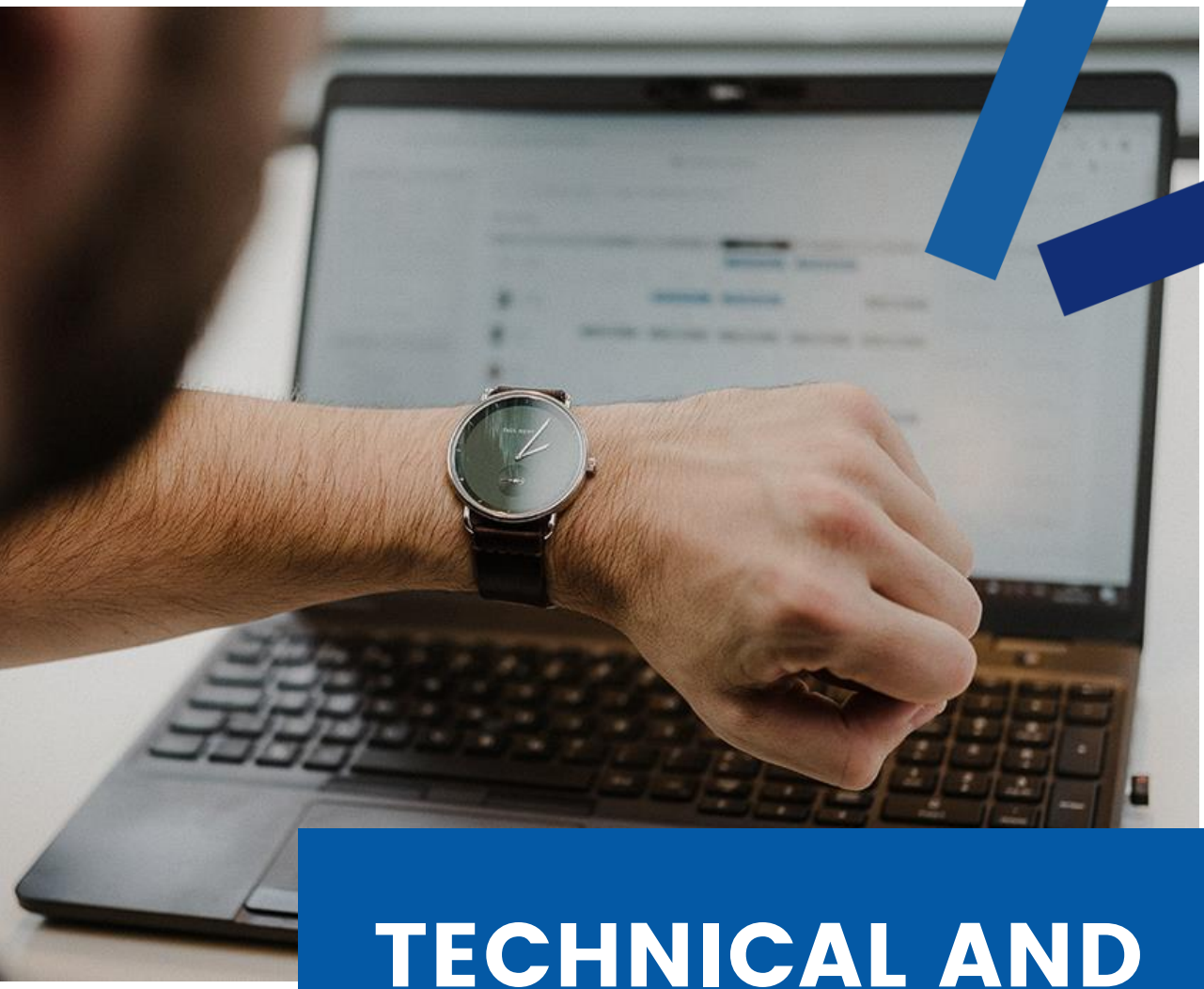
protime



TECHNICAL AND ORGANIZATIONAL MEASURES

Introduction

In today's ever-evolving threat landscape, protecting your company's sensitive data and assets from cyberattacks has become more critical than ever. This is especially true for Software-as-a-Service (SaaS) companies, which store and process their customers' data on the cloud.

To ensure the security and confidentiality of our customers' data, our Protime has implemented a comprehensive set of technical and organizational measures. In this document, we will provide an overview of the measures we have taken to safeguard our customers' data from potential threats.

By implementing these measures, we aim to provide our customers with the highest levels of security and trust in our SaaS offering. We believe that transparency and proactive risk management are essential to building and maintaining strong relationships with our customers, and we are committed to continuously improving our security practices to stay ahead of emerging threats.

Measures

Information Security Policy and Organization of Information Security	**Ownership for Security and Data Protection**. Protime has appointed a Risk & Security Officer responsible for coordinating and monitoring the security rules and procedures as well as data protection compliance. **Security Roles and Responsibilities**. Security responsibilities of Protime co-workers are formally documented and published in security and privacy policies. **Risk Management Program**. Protime executes periodical risk assessments of the implemented security controls.
Human Resources Security	**Confidentiality obligations**. Protime co-workers are subject to confidentiality obligations and these are integrated into employment contracts. **Termination.** Protime ensures according to formal security administration procedures that access rights are timely revoked upon termination.
Asset Management	**Asset Inventory**. Protime maintains an inventory of all computing equipment and media used. Access to the inventories is restricted to authorized Protime personnel. **Asset Handling.** Protime has procedures for securely disposing of media and printed materials that contain confidential data.
Information Access Control	**Access Policy.** Protime enforces an access control policy based on need-to-know and least privileges principles. **Access Authorization** - Protime has implemented and maintains an authorization management system that controls access to systems containing Personal Data. - Every individual accessing systems containing Personal Data has a separate, unique identifier/username. - Protime restricts access to Personal Data to only those individuals who require such access to perform their job function. - Technical support personnel are only permitted to have access to Personal Data when needed. **Authentication**

	- Protime uses industry standard practices to identify and authenticate users who attempt to access Protime network or information systems, including strong authentication. - Where authentication mechanisms are based on passwords, Protime requires that the passwords are renewed periodically and that they are at least eight characters long and sufficiently complex. - De-activated or expired identifiers/usernames are not granted to other individuals. - Accounts will be locked out in case of repeated attempts to gain access to the information system using an invalid password. - Protime maintains practices designed to ensure the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.
Physical and Environmental Security	**Physical Access to Facilities.** - Protime limits access to facilities where information systems that process Personal Data are located to identified authorized individuals. - Physical access to data centers is only granted following a formal authorization procedure, and access rights are reviewed periodically Protection from Disruptions. Protime uses a variety of industry standard systems to protect its data centers against loss of data due to power supply failure and fire.
Operations Security	**Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no data has been updated during that period), Protime maintains backup copies of Personal Data for recovery purposes. - Protime stores copies of Personal Data and data recovery procedures in a different place from where the primary computer equipment processing the Personal Data is located. Malicious Software. Protime maintains anti-malware controls to help avoid malicious software gaining unauthorized access to Personal Data. Data Beyond Boundaries. Protime standardly encrypts, or provides the mechanisms to the Client to encrypt, Personal Data that is transmitted over public networks. Event Logging. Protime logs access and use of its information systems containing Personal Data, registering the access ID, time and relevant activity.
Communications Security	**Network Segregation.** Protime has implemented a network segmentation policy and controls to avoid individuals gaining access to systems for which they have not been authorized. **Information Transfer.** Any transfer of Personal Data to third parties is only performed following the execution of a formal written non-disclosure agreement.
System Acquisition, Development & Maintenance	**Security Requirements.** Requirements for protecting data and systems are analyzed and specified. **Change Control.** Protime has implemented a formal change management process to ensure changes to operational systems and applications are performed in a controlled way.
Supplier Relationships	**Supplier Selection.** Protime maintains a selection process by which it evaluates the security, privacy and confidentiality practices of a Sub-processor in regard to data handling.

	Contractual Obligations. Suppliers with access to Personal Data are subject to data protection and information security obligations, and these are formally integrated into supplier contracts.
Information Security Incident Management	Protime maintains a record of security breaches with a description of the breach, the time, the consequences of the breach, the name of the reporter and to whom the breach was reported.
Business Continuity Management	**Disaster Recovery.** Protime maintains a disaster recovery plan for the facilities in which Protime information systems that process Personal Data are located. **Redundancy.** Protime's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Data in its original or last-replicated state from before the time it was lost or destroyed.
Compliance	**Security Reviews.** Information security controls are independently audited and reported to management on a periodical basis.