sodexo
QUALITY OF LIFE SERVICES

General Data Privacy Regulation

Technical and Organisational Measures

Overview

SODEXO IT GENERAL CONTROLS

Contents

Introduction

This document describes the technical and organizational security measures implemented by Sodexo as part of the IT General Controls.

Additional controls may be applied to individual applications.

Security Framework

Sodexo understands that the confidentiality, integrity and availability of information is essential to our customers' operations and their trust in us as a service provider.

Our information security program leverages the ISO/IEC 27000 control standard as its baseline and applies the appropriate access controls and other protocols that help us prevent, detect and respond to incidents of inappropriate data handling within our company.

Roles and responsibilities for Information Security are clearly defined in the Group Information and Systems Security Policy which is written and maintained by the Group CISO.

Security Policy

Sodexo's information security policies and procedures are made available to all Sodexo personnel. They are reviewed on a regular basis and updated as appropriate for accuracy, completeness and applicability. Sodexo's information security principles include:

› Human Resources Security Policy

› Asset Management

› Access Control

› Physical Security

› Operations and Communications Security

› System acquisition, development and maintenance

› Third Party Relationships

› IS&T Security Incident Management

› Disaster Recovery Plan

› Compliance

Access Control of Processing Areas (Physical)

Suitable measures are implemented in order to prevent unauthorized persons from **gaining access** to the data processing equipment.

Entrances to the data centres are secured 24 hours a day, 7 days a week with security officers, an access control system, physical barriers and video monitoring.

Critical IT equipment (such as servers, routers) is stored in physical areas that meet standards in terms of protection against fire, electrical surge, flooding or other natural disasters.

Computer storage rooms contain adequate back-up power supplies, air conditioning and fire detection/suppression means.

Access to the data centre and computer rooms is limited to authorized personnel and physically secured.

Visitors are required to present a valid photo ID, are admitted only if they have approval and are issued a temporary identification badge requiring escort while in the facility.

Access Control to Data Processing Systems (Logical)

Suitable measures are implemented to prevent the data processing system from **being used** by unauthorized persons.

All access rights are granted and removed according to a formal User Access Management (UAM) process (new users, job changes, termination).

Access to the Sodexo network, critical applications and databases is granted upon a formal and documented request, approved by the process, application or data owner at appropriate level. The requests are processed by the appropriate team.

Access rights are reviewed on a regular basis and signed off by process, application or data owner. Upon termination of a user, access rights are promptly removed or deactivated.

Access to the system is protected by passwords which are sufficiently long and sophisticated; periodically changed; resistant to intrusion attempts and appropriate for the nature of the system, data and user account.

Additional practices from the Group Information and Systems Security policy are implemented including higher complexity for administration accounts.

Access Control to Use Specific Areas of Data Processing Systems

Suitable measures are implemented to prevent **access to Personal Data** by unauthorized persons.

Production systems are on separate environments from development and test systems.

Persons entitled to use the data processing system are only able to access Personal Data within their scope and to the extent covered by their respective access permission / roles (authorization).

IT personnel only perform authorized activities appropriate to their job responsibilities through adequate segregation of roles and responsibilities and logging of sensitive activities.

Availability Control

Suitable measures are implemented to ensure that Personal Data is protected from **accidental destruction or loss**.

Data and programs are properly backed up according to the nature and classification of the data, risk of loss and requirements for recovery. Backups of data / databases are performed at least once a day on physical media (hard disk, tapes, and storage area networks).

Testing is conducted periodically to ensure that in the event of an incident (data corruption, program errors, hardware failure, virus infection, IT attacks, etc.), the application and database servers can be effectively restored from the backups.

An IT disaster recovery plan exists to effectively reduce the impact of major disruption on key business functions and processes based on the major risks identified and the business requirements for resuming operations.

Management has identified data files that must be retained to comply with local regulatory requirements and the appropriate process to do so is in place.

An archiving solution has been identified which allows for access to and recovery of historical data, either electronically or manually. The archiving / purge procedures are defined and performed regularly by individuals identified. Audits of volumes, performance, and response times are also regularly performed.

Transmission Control

Suitable measures are implemented to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties **during the transmission** of the data.

Interfaces have automated, semi-automated or manual controls such that data transmission or processing through interfaces (or data transfer) is accurate, complete, timely, authorized and auditable.

Maintenance and monitoring

Measures are implemented to ensure that the system is **free from major known vulnerabilities** and to prevent manipulation by **malicious programs or individuals.**

Access to Sodexo information system (networks, systems, hardware, files, etc.) is monitored through appropriate use and configuration of firewalls, detection and auditing of unauthorized access attempts, analysis of security incident reports.

Recommended and applicable security configurations from the vendors, professional organizations and the Group are adopted, documented and then followed.

There is a periodical review performed to ensure that security parameters remains aligned with security recommendations.

Anti-virus and anti-malware software is used to protect the system.

Changes to business application programs, configurations, databases, operating system, IT infrastructure and processes are evaluated, prioritized, authorized, performed and documented in a formal structured manner so as to reduce the risk in integrity, security and availability of system and data.

Compliance

Measures are implemented to ensure that persons employed by Sodexo and other persons at the place of work, are **aware of and comply** with the technical and organizational measures set forth in this document.

Sodexo keeps documentation of technical and organizational measures in case of audits and for the conservation of evidence.

Sodexo may make non-confidential portions of audit reports available to customers to verify compliance with the technical and organizational measures.

Sodexo closely monitors its partners and vendors, including periodic review of the security controls, through on-site audits, attestation reports / certificates and questionnaires where applicable.