odaseva

ODASEVA SECURITY CONTROLS

1. Introduction

Security is at the core of Odaseva. In order to provide the highest degree of security and availability for the platform and SaaS services, Odaseva established and currently maintains a variety of policies, procedures and controls covering administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data uploaded to the SaaS services.

The measures defined in this document are based on best practices and industry standards, i.e., NIST 800-53, and include areas covering infrastructure monitoring and security operations, risk management, communication process and rigorous management of access rights to information of its information system. Odaseva reserves the right to update these controls over time provided that updates will not materially decrease the overall security of the SaaS services during a subscription term.

2. Encryption

As a no-view provider, Odaseva uses multiple layers of state of the art encryption to protect customer data. Odaseva employees, administrators, and third party cloud providers do not have the ability to view customer data in clear text.

2.1. Customer data is granularly encrypted at the field and file level with the customer's provided AES-256 bit data encryption key.

2.2. Customers are given the choice between two key management solutions:

2.2.1. Bring Your Own Key - Odaseva stored
- Encryption key is managed by the customers through the Odaseva platform.
- Keys are stored encrypted and separate from systems storing processed data.
- Keys are retrievable in the event of loss through Odaseva emergency key loss process and break-glass procedure.

2.2.2. Bring Your Own Key Management System (KMS) Option
- Encryption key is managed by the customers on their own KMS.
- Customers have full control access to keys and may revoke access at any time.
- Key usage activities are logged on customer's KMS.
- Keys cannot be recovered by Odaseva in the event key is lost.

2.3. Any integration or system access, in particular those concerning Odaseva platform, will be implemented exclusively through state of the art TLS protocols (TLS1.2 or greater).

3. Access, Identification, and Authentication

Access to Odaseva's data and information systems is granted to individuals based on the principle of least privilege and need-to-know. Employees, contractors, or third parties are only granted access if it is required to perform job responsibilities.

3.1. Odaseva controls access to information, information assets and business processes based on business and security requirements.

3.2. Policies and procedures for account and access management have been established, documented, and reviewed based on business and security requirements.

3.3. Odaseva ensures authorized user accounts are registered, tracked, and periodically validated to prevent unauthorized access to information systems.

3.3.1. There is a formal documented and implemented user registration and deregistration procedure for granting and revoking access

3.3.2. Privileged access includes any accounts or privileges that provide the user escalated access and rights to the information resource. The allocation and use of privileges to information systems and services are restricted and controlled.

3.3.3. Privileged access includes any accounts or privileges that provide the user escalated access and rights to the information resource. The allocation and use of privileges to information systems and services are restricted and controlled.

3.3.4. Odaseva has set up a standard for the creation of strong passwords, the protection of those passwords, the prevention of their reuse, and the frequency of change. Passwords are controlled through a formal management process.

3.3.5. A formal record of all users registered and approved to use a system or service is maintained. All access rights are regularly reviewed by management via a formal documented process.

3.3.6. Odaseva has implemented segregation of duties for management of sensitive systems.

3.4. Odaseva prevents unauthorized access to operation systems.

3.4.1. All users have a unique identifier (user ID) for their personal use only, and authentication techniques are implemented to substantiate the claimed identity of a user. Generic accounts are not used.

3.4.2. Odaseva has implemented Role Based Access Control (RBAC) and access to systems is given on a need to know basis.

3.4.3. Systems for managing passwords are interactive and ensure quality passwords.

3.4.4. Multi-factor authentication is mandatory for all Odaseva employees and contractors accessing Odaseva information system.

3.4.5. Inactive sessions are shut down after a defined period of inactivity.

3.4.6. Maximum number of failed login attempts and lockout duration is enforced.

3.5. Odaseva ensures the security of information when using mobile computing devices and teleworking facilities.

3.5.1. Zero trust network access has been implemented for remote access to internal applications.

3.5.2. A formal policy is in place, and appropriate security measures (e.g., full-disk encryption, anti-malware, etc.) are adopted to protect against the risks of using mobile computing and communication devices.

3.5.3. End user devices are centrally managed and compliance enforcement is enabled for access to sensitive systems.

3.5.4. Policies, operational plans, and procedures are developed and implemented for teleworking activities.

3.6. Odaseva ensures access to the platform is granted to authorized customers only.

3.6.1. User accounts are linked to individual users of customers.

3.6.2. User account password follows strict requirements for length and complexity with period of validity and password history enforced.

3.6.3. Maximum number of failed login attempts and lockout duration is enforced.

3.6.4. Multi-factor authentication is available for accessing the Odaseva platform.

3.6.5. Customers can enable delegated single sign-on via their Salesforce instance.

3.6.6. Customer’s administrators can manage the provisioning and deprovisioning of users and associated access as needed.

3.6.7. Role-based access controls are provided to customers to manage the permissions granted to their users.

4. Security Awareness and Training

4.1. All workforce members receive appropriate training concerning the Company's security policies and procedures. Such training is provided as part of employees onboarding and repeated annually.

4.2. Attendance and/or participation in such training is mandatory and is documented.

4.3. Latest versions of the security policies and measures are made available to all employees.

4.4. Specific training based on roles (secure coding, privileged users training, etc.) is delivered on an ongoing basis to respond to environmental and operational changes impacting the security of the organization.

4.5. Security reminders are sent to all employees. These reminders may address password security, malicious software, incident identification and response, access control, etc. These reminders can come through formal training, e-mail messages, discussions during staff meetings, or intranet articles.

4.6. Distribution of special notices providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures are communicated.

4.7. Phishing exercises are conducted on at least an annual basis.

5. Audits Logging and Monitoring

Odaseva analyzes and correlates audit records across different repositories using a security information and event management (SIEM) tool or log analytics tools for log aggregation and consolidation from multiple systems, applications, and devices.

Odaseva ensures information security events are monitored and recorded to detect unauthorized information processing activities in compliance with all relevant legal requirements.

5.1. Audit logs recording users and administrators activities, exceptions, and information security events are produced and kept for an agreed period to assist in future investigations and access control monitoring.
5.2. Procedures for monitoring use of information processing systems and facilities are established to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed regularly.
5.3. Automated rules are in place to generate alerts for suspicious or abnormal behaviors. These alerts are regularly reviewed by Odaseva Security personnel.

6. Security Assessment and Vulnerability Management

Timely information about technical vulnerabilities of information systems being used is obtained, Odaseva's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

6.1. Odaseva hires independent third-party penetration testers to perform both network and web vulnerability assessments on the platform at least two times per year. For added security, penetration tests are performed by two separate vendors. The scope of these audits includes compliance against the Open Web Application Security Project (OWASP) Top 10 Web Vulnerabilities (www.owasp.org).
6.2. Odaseva performs periodic static code analysis assessments as part of its continuous monitoring program to help ensure application security controls are properly applied and operating effectively.
6.3. Vulnerabilities related to information and related assets are proactively identified through automated vulnerability scans and remediated according to the risk.
6.4. Vulnerabilities that pose a critical information risk are prioritized and patched early.

7. Configuration management

7.1. Odaseva ensures that operating procedures are documented, maintained, and made available to all users who need them.
7.2. Systems are configured according to industry security baselines such as CIS Benchmarks.
7.3. Odaseva has established requirements governing the installation of software, enforce software installation restrictions and monitor compliance on a continual basis.
7.4. Critical systems are monitored with file integrity monitoring and intrusion detection technologies.
7.5. Changes to information assets and systems are controlled and archived.
7.6. Segregation of duties is enforced to reduce opportunities for unauthorized or unintentional modification or misuse of Odaseva's assets.

8. Business Continuity Management and Disaster Recovery

8.1. Odaseva ensures that strategies and plans are in place to counteract interruptions of business activities and to protect critical business processes from the effects of major failures of information systems or disasters, and to ensure their timely resumption.
    8.1.1. Events that can cause interruptions to business processes are identified, along with the probability and impact of such interruptions and their consequences for information security.
    8.1.2. Plans are developed and implemented to maintain or restore operations and to ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
    8.1.3. A single framework of business continuity plans is maintained to ensure that all plans are consistent, to consistently address information security requirements and to identify priorities for testing and maintenance.

8.2. Odaseva leverages leading cloud service providers globally, inheriting the 99.9% availability of these providers. Odaseva's data storage architecture provides customers with a 99.999999999% of data durability.

8.2.1. Customer data is processed and stored encrypted across multiple availability zones.

8.2.2. Versioning is used to preserve, retrieve, and restore previous version of customer data backups, hence providing immutability.

8.2.3. Regular back-up copies of information and software are made and secured.

9. Information Security Incident Management

Odaseva has implemented an incident response plan to detect, respond to, and recover from security incidents. The company will regularly test the incident response plan to ensure it is effective. The goal of incident management is to reduce the risk inherent to securing information systems and information assets, and to mitigate any harmful events from the possible exploitation of vulnerabilities.

9.1. Odaseva ensures that information security events and weaknesses associated with information systems are handled in a manner allowing timely corrective action to be taken.

9.2. Information security events are reported to the Odaseva security team. All employees, contractors, and third-party users are made aware of their responsibility to report any information security events as quickly as possible.

9.3. Odaseva ensures a consistent and effective approach to the management of information security incidents.

10. Information Exchange and Protection

10.1. Odaseva protects the information it owns or possesses in its custody based on the nature of the information and the risk exposure to Odaseva, its workforce members, its customers, and its directors from inappropriate or undesired access, disclosure, or destruction. Odaseva prevents unauthorized disclosure, modification, removal or destruction of information assets, or interruptions of business activities.

10.2. Multiple safeguards are formally addressed prior to allowing the use of information systems for information exchange. Odaseva ensures the exchange of information within an organization and with any external entity is secured, protected, and carried out in compliance with relevant legislation and exchange agreements.

10.3. Formal policies, procedures, and controls are in place to protect the exchange of information using all types of communication mediums.

11. Physical and Environmental Protection

11.1. Odaseva policies require adequate physical safeguards to include both facility access controls, fire and natural disaster protection, and device and media controls to secure information systems and information assets.

11.2. Odaseva leverages trusted cloud providers to comply with these requirements and does not host any servers / network devices on Odaseva premises.

11.3. Physical protection and guidelines for working in areas are designed and applied.

12. Program Management and Security Policy

Odaseva has implemented and manages an ISMS aligned with ISO27001 guidelines.

12.1. The information security management system (ISMS) establishes the overall information security and protection program that is intended to complement the other security policies. The ISMS is formally documented, approved, actively monitored, reviewed, and updated to ensure that program security

objectives are met. The ISMS sets up access controls that limit access to sensitive systems and information to the minimum necessary level to support organizational service delivery.

12.2. The information security policy and procedures are intended to ensure the confidentiality, integrity, and availability of information in any form created, received, maintained, or transmitted.

12.3. Management provides the direction for business objectives and relevant laws and regulations and demonstrates support for and commitment to information security through the issue and maintenance of information security policies across Odaseva.

13. Personnel Security

Odaseva ensures that employees, contractors, and third-party users are suitable for the roles for which they are being considered to reduce the risk of fraud, theft, or misuse of facilities.

13.1. Background verification checks on all candidates for employment, contractors, and third-party users are carried out in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

13.2. Odaseva ensures agreements are signed by employees, contractors, and third-party users of information assets on their security roles and responsibilities at the time of their employment or engagement, prior to sensitive access being granted.

13.3. Management requires employees, and where applicable, contractors and third-party users, to apply security in accordance with established policies and procedures of Odaseva.

13.3.1. All employees, contractors, and third-party users of Odaseva receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

13.3.2. There is a formal disciplinary process for employees who have violated security policies and procedures.

13.4. The access rights of all employees, contractors, and third-party users to information and information assets are removed upon termination of their employment, contract, or agreement, or adjusted upon a change of employment (i.e., upon transfer within Odaseva).

14. Personally Identifiable Information Processing and Transparency

14.1. A Data Protection Officer is appointed and is responsible for the development, implementation, and maintenance of policies, procedures, and processes regarding continuing compliance with privacy regulations such as GDPR, CCPA and the HIPAA Privacy Rule.

14.2. Odaseva ensures that PII is used solely for the purpose(s) specified in the privacy policy and only for a purpose that is compatible with the purpose for which the PII was collected.

14.3. The use and disclosure of PII for specific purposes are limited to explicit and legitimate purposes and must fulfill the stated purpose(s) or to abide by applicable laws.

14.4. Odaseva privacy policy is published and available at: https://www.odaseva.com/assets/pdf/Odaseva-Privacy-Policy.pdf

15. Risk Management Program

A risk management strategy is developed and managed by management and documented in the risk management program. The risk management strategy defines Odaseva's risk tolerance, risk mitigation techniques, and risk assessment methodology.

15.1. Odaseva has developed and maintains a risk management program taking into account security needs and objectives, in order to identify risks and mitigate them in a timely manner.

15.2. Risks are continually evaluated and assessed, through threat monitoring and internal audits.

16. Asset Management

16.1. All assets, including information, are clearly identified and an inventory of all assets drawn up and maintained.
16.2. Rules for the acceptable use of information and assets associated with information processing systems are identified, documented, and implemented.
16.3. Information is classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.

17. Network Security

Network security is considered throughout the complete hardware and software lifecycle. Controls are implemented to ensure the security of information and the protection of connected services in terms of confidentiality, integrity, and availability. Appropriate logging and monitoring are applied to enable recording and detection of actions that may affect, or are relevant to, information security. Odaseva ensures the protection of information in networks and protection of the supporting network infrastructure.

17.1. Networks are managed and controlled to protect Odaseva from threats and to maintain security for the systems and applications using the network, including information in transit.
17.2. Odaseva prevents unauthorized access to networked services.
  17.2.1. Appropriate authentication methods are used to control access by remote users including requirements of multifactor authentication
  17.2.2. Groups of information services, users, and information systems are segregated on Odaseva's networks. Development environments are strictly separated from production instances.
  17.2.3. Sensitive systems are dedicated and located in isolated computing environments.
  17.2.4. Firewalling is in place to ensure that computer connections and information flows do not breach the access control policy of the business applications.

18. Secure Software Development and Information Security

Odaseva ensures the security of application system software and information throughout the development process, and project and support environments are strictly controlled.

18.1. Evolutions and enhancements of Odaseva platform go through a threat modeling process to identify threats and specify security controls.
18.2. Secure development guidelines are maintained and distributed to the development team. Formal training on secure coding is in place.
18.3. The implementation of changes, including patches, service packs, and other updates and modifications, are controlled using a formal change control procedure, including following manual and automated code review and in-depth QA testing.
18.4. If any, outsourced software development is supervised and monitored by Odaseva.
18.5. Changes are communicated through release notes published on the Odaseva platform.

19. Third Party Risk Management

Odaseva ensures that third-party service providers maintain security requirements and levels of service as part of their service delivery agreements.

19.1. Odaseva has implemented a supplier management program. New third parties must go through a validation process covering contractual and security requirements.
19.2. Odaseva identifies and mandates information security controls to specifically address supplier access to Odaseva's information and information assets
19.3. Odaseva ensures that the security controls, service definitions, and delivery levels included in the third-party service delivery agreement are implemented, operated, and maintained by the third party.

20. Compliance and independent external audits

20.1. Odaseva ensures that all information systems adhere to all applicable laws, statutory, regulatory, or contractual clauses, and any business or security requirements.

20.2. Odaseva is ISO/IEC 27001:2013 certified

20.3. Odaseva undergoes an annual SOC2 Type II audit under SSAE-18 to independently verify the effectiveness of its information security practices, policies, procedures, and operations for the following Trust Services Criteria: Security, Availability, and Confidentiality.

20.4. Odaseva leverages leading global SaaS and cloud service providers for its web application, computing and storage for the Odaseva platform. AWS and Azure are top-tier facilities with several accreditations, including SOC1 - SSAE-18, SOC2, ISO 27001, and HIPAA.