OptiMiser Information Security Policy

Last update November 29, 2025

Purpose

This document defines the data security policy of OptiMiser, LLC. OptiMiser takes the privacy of our clients and partners very seriously. To ensure that we are protecting our corporate and client data from security breaches, this policy must be followed and will be enforced to the fullest extent.

Scope

This policy applies to all data managed or received by OptiMiser, including electronic information found in email, remote or local databases, applications, and other media; paper information, such as hard copies of electronic data, employee files, internal memos, and so on. It is inclusive of data outside of OptiMiser stored in a cloud service, and/or held on a mobile computing device.

Applicability

This policy applies to all OptiMiser employees, contractors, partners, management, and vendors who have access to any of the data described in the Data Types section below. All covered individuals hereinafter described as “Team Members,” regardless of whether they are OptiMiser employees or contractors.

Management

Ownership of this policy falls to OptiMiser’s Management Team, Andy Bardwell and Larry Hausman-Cohen. For any questions about this policy, or to report misuse of corporate or personal data, please contact one of these Management Team members. This team will work to maintain data access privileges, which will be updated as required when a Team Member joins or leaves the company. Compliance with this policy will be monitored by all Management Team members.

Data Types

OptiMiser deals with two main kinds of data, both of which are covered by this policy:

1. **Company-owned data** including corporate financials, employment records, payroll, and client data (including address and audit data) received by OptiMiser and not owned by an OptiMiser partner or client, and all OptiMiser intellectual property (IP);
2. **Private data** that is the property of our clients or partners including credit card information, proprietary information or IP not owned by OptiMiser, and address or audit information not owned by OptiMiser. This information always remains the property of the client or partner.

Data Classifications

OptiMiser’s data is comprised of three classifications of information:

1. **Public/Unclassified.** This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available, and can be distributed as needed. Public/unclassified data includes but is not limited to marketing materials, corporate financials or legal documents that are widely published, and educational materials that are freely available.

   Team Members may send or communicate a public/unclassified piece of data with anyone inside or outside of the company.

2. **Private.** This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific Team Members or groups, and cannot be distributed outside of OptiMiser

without written permission by a Management Team member or a non-disclosure agreement with the party receiving the information. Private data includes, but is not limited to, company financials, policies, or legal documents that are not widely distributed; OptiMiser marketing or development strategy; or information about OptiMiser's method of operation.

All information not otherwise classified will be assumed to be Private.

3. **Confidential.** This is defined as personal or corporate information that may be considered potentially damaging if released and may only be accessible to specific Team Members. Confidential data includes, but is not limited to, addresses or home audit data; personal contact information for homeowners; tax forms; accounting data; security procedures not widely distributed; all software code or information about the development of OptiMiser products (to the extent this information is not widely available); all confidential intellectual property or trade secrets owned by OptiMiser or its partners; all data or other information received by OptiMiser partners or clients subject to a non-disclosure agreement or otherwise designated as confidential; and credit card information. OptiMiser considers it a top priority to protect the privacy of our clients and employees; A separate privacy policy (https://www.omaudits.com/privacy-policy) outlines our commitment to protecting personal data.

   Access to confidential information owned by OptiMiser is generally limited to those Team Members who must have access to the information for their work with OptiMiser (the Working Team). This information may only be distributed beyond the Working Team, *regardless of whether such distribution is to OptiMiser Team Members*, pursuant to a properly-executed non-disclosure agreement with the party receiving the information. *To the extent any confidential data is owned by a party other than OptiMiser, this information may only be disclosed per written permission by an authorized agent of that party.*

   It is the responsibility of everyone who works at OptiMiser to protect this information. Even unintentional abuse of private or classified data will be considered punishable in accordance with the extent and frequency of the abuse.

   Private Data must be encrypted with minimum 256-bit cryptography while on our servers.

Responsibilities

All Team Members are responsible for adhering to the policy and reporting any activities that do not comply with this policy.

The Management Team is responsible for ensuring that all OptiMiser Team Members understand the scope and implications of this policy, and that a signed copy of the most current policy is kept on file for each Team Member.

The Management Team will periodically monitor data for any unauthorized activity and are responsible for updating access requirements as needed.

Any Team Member who authors or generates corporate or client data must classify that data according to the criteria outlined above.

Implemented Security Measures

All OptiMiser Product Development and Delivery Team Members (all personnel with access to Private information) Team Members are responsible for implementing the following data security measures, to the extent applicable to the scope of their work with OptiMiser:

1. Describe access controls (User Account Administration Policy)
2. Describe segregation of duties
3. Describe password standards (User Account Administration Policy)
4. Self-monitoring for acceptable data use
5. Reporting security breaches immediately to a Management Team Member (Information Security Incident Reporting)

6. Reporting data use or access in violation of this policy by any other Team Member (Information Security Incident Reporting)

Background Checks

OptiMiser LLC will obtain one or more consumer reports or investigative consumer reports (or both) about its employees and contractors dealing with private and/or confidential data. The reports will include information about their character, general reputation, personal characteristics, and mode of living.

We will obtain these reports through a consumer reporting agency. Our consumer reporting agency is backgroundchecks.com ("BGC"). BGC's address is P.O. Box 353, Chapin, SC 29036. BGC's telephone number is (866) 265-6602. BGC's website is www.backgroundchecks.com, where you can find information about BGC's international privacy practices.

To prepare the reports, BGC may investigate education, work history, professional licenses and credentials, references, address history, social security number validity, right to work, criminal record, lawsuits, driving record, credit history, and any other information with public or private information sources.

All employees and contractors with access to private and/or confidential data must acknowledge receipt of the above disclosures and consent to the background check.

Training and Review

All Team Members must review this policy and receive training in any applicable information security measures when they join OptiMiser, and as needed as security measures may change. Trainings will be coordinated and run by the Management Team.

Notice and Acknowledgement

All Team Members are required to acknowledge this policy when first contracting with OptiMiser. As the policy may change from time to time, all Team Members will be notified, and will be required to reaffirm acknowledgement of the modified policy.

Review

The Management Team is responsible for keeping this policy current. This policy will be reviewed with legal counsel annually or as circumstances arise, and will be updated as needed to reflect new legal or practical requirements.

Enforcement

Failure to comply with any aspect of this policy will be grounds for immediate termination of a working relationship with OptiMiser, including termination of any existing contract, and will be reported promptly to any appropriate legal authority and to any OptiMiser business partner affected by the policy violation.

Acknowledgement

I agree to the terms and conditions set forth in this policy:

Ryan Moore, COO

11/29/2025