Meier Made, LLC

Information Security Policy

How Meier Made protects information and supports secure, client-hosted platform integrations.

Effective September 7, 2026

Purpose and scope

This policy establishes the information security requirements of Meier Made, LLC for its personnel, contractors, automation, developer applications, and authorized access to client systems. It supports the protection of company information and client-authorized advertising, commerce, financial, and other platform data.

These requirements guide our work; they are not a certification or an assertion that every client system implements identical controls. Platform questionnaires must describe the actual deployment and supporting evidence. Applicable law, platform obligations, and written client agreements govern any additional requirements.

Client-hosted integrations

Meier Made develops and maintains integrations that enable clients to transfer authorized platform data into their designated data warehouses. Integration workloads run exclusively in client-controlled infrastructure. Meier Made does not host client data pipelines.

Clients authorize the applicable developer application through the platform-supported authorization process. The client deployment uses the permitted access to retrieve data and deliver it to the client-designated destination. Authorization does not grant permission to access unrelated accounts or use data for unrelated purposes.

Meier Made may have client-authorized access for deployment, administration, maintenance, and troubleshooting. Client-hosted does not mean that Meier Made cannot access data. Such access remains subject to the same confidentiality, least-privilege, and data-handling requirements as other client work.

Governance and responsibilities

Andrew Meier owns this policy, approves access and security exceptions within Meier Made's authority, coordinates incident response, and reviews material security risks. Personnel and contractors must follow this policy and the obligations of the engagement before accessing client information.

Meier Made is responsible for the security of its developer applications, code changes, company accounts, and authorized support activities. Clients control their infrastructure, platform accounts, and data destinations. The engagement must identify responsibility for administration, monitoring, retention, backups, recovery, and incident coordination. Client ownership does not remove Meier Made's responsibilities for its own actions.

Data classification and permitted use

Public information may be shared when approved. Internal business information is restricted to business use. Client datasets, private code, and non-public platform information are confidential. Credentials, authorization tokens, and sensitive personal information require restricted access and handling appropriate to their sensitivity.

Retrieve only the accounts, fields, and time ranges needed for the client-authorized purpose. Advertising metrics must not be assumed anonymous, and commerce or financial datasets may contain personal information. Meier Made does not sell client or platform data or use it for unrelated purposes.

Keep client datasets in client-approved systems. Troubleshooting must use the minimum necessary information and prefer redacted examples. Do not copy client records into company tickets, communications, or AI tools without client authorization and an approved handling basis.

Identity and access control

Grant access only to authorized people and workloads for a defined business need. Use individual identities for people and scoped service identities for automation; separate administrative, deployment, and runtime permissions where applicable. Review access when responsibilities change and remove it when no longer needed.

Require multi-factor authentication for human access to administrative and sensitive systems where supported. Systems that cannot meet this requirement need a documented alternative or exception. Workload authentication uses restricted credentials or platform-supported identity mechanisms, not shared human accounts.

Application authorization and credentials

Use platform-approved authentication and request only permissions needed by the integration. Configure authorized callback destinations and protect authorization flows against unintended access. Never request a client's third-party account password as a substitute for delegated authorization.

Protect developer-app credentials and client-specific tokens in approved secret-management or credential-storage facilities. Limit access to required operators and workloads. Do not expose secrets in source code, URLs shared for support, logs, screenshots, or messages. Revoke or rotate credentials when compromise is suspected or access is no longer authorized; handle expiration and revocation without bypassing platform controls.

Infrastructure and network protection

Deploy integrations only in the approved client environment and separate client access, credentials, and data destinations. Restrict administrative interfaces and network access to the intended users, services, and connections. Do not expose databases, credential stores, or administration endpoints publicly without an explicitly approved access design.

Use encrypted transport for platform requests and data transfers, and approved storage encryption for persisted confidential information. Apply security updates and review infrastructure changes according to risk. The specific network segmentation, firewall, and monitoring controls must be assessed in the client deployment rather than inferred from this policy.

Secure development and change management

Maintain application, connector, and infrastructure changes in version control. Review and test changes before production delivery, including authorization, data handling, and credential exposure where relevant. Restrict production deployment access and use the engagement's approved delivery process.

Assess dependencies and reported vulnerabilities, prioritize remediation by risk and exposure, and retain enough change history to investigate issues and recover from failed changes. Do not bypass a required review or security control to expedite a deployment.

Logging and monitoring

Use access, application, and infrastructure events appropriate to the engagement to identify failures, suspicious activity, and unauthorized access. Assign monitoring and escalation responsibilities explicitly; this policy does not represent a dedicated round-the-clock security operations service.

Restrict access to logs and diagnostics, retain them according to the approved purpose, and avoid recording secrets or unnecessary personal data. Redact sensitive information before sharing diagnostic evidence outside the approved client environment.

Incident response

Promptly report suspected credential exposure, unauthorized access, data loss, or other security concerns to the policy owner. Assess the affected systems and information, contain the issue, preserve appropriate evidence, investigate the cause, and coordinate recovery with the client and relevant providers.

Notify affected clients, platforms, and authorities as required by applicable agreements, platform rules, and law. Do not assume one notification deadline applies to every integration. Record the response and corrective actions, verify recovery, and update controls after material findings.

External reports may be sent to info@meiermade.com with the subject Security report. Do not include credentials or customer records in the initial message. Our public security-reporting page describes the reporting process and acknowledgment target.

Retention, deletion, and offboarding

Set data retention and deletion responsibilities with the client according to authorized use, applicable law, and platform obligations. On termination or revocation, stop unauthorized future access, remove unneeded credentials and support permissions, and coordinate disposition of stored information with the client.

Revoking an application's authorization does not necessarily delete data already synchronized into a warehouse. Address active data, logs, temporary files, and backup expiration separately. Follow the published data-deletion process for requests to Meier Made, verify the requester's authority, and coordinate actions in client-controlled systems with the client.

Backup and recovery

Identify the owner, scope, retention, and recovery expectations for client-hosted workloads and data before production use. Configure and validate backups and restoration where assigned to Meier Made by the engagement. Do not treat source control or a provider's storage durability as a substitute for a data recovery plan.

Document any agreed recovery objectives and dependencies. Client hosting alone does not establish a backup guarantee, and Meier Made does not promise a universal recovery time or recovery point across engagements.

Third parties and personnel safeguards

Assess third-party tools and services for their intended use, access, and handling of confidential information. Disclose or obtain approval for subprocessors where required by the client agreement or platform rules. Do not send client data to a new service simply because the service is available.

Personnel must protect devices with access controls, supported security updates, screen locking, and storage encryption appropriate to the information accessed. Provide security expectations when granting access and reinforce them when responsibilities or risks change. Report lost devices, phishing, and suspected compromise promptly.

Exceptions and policy review

Security exceptions require the policy owner's approval and, where applicable, client approval. Record the reason, risk, compensating safeguards, responsible owner, and review or expiration date. An exception cannot override applicable law or platform obligations.

Review this policy at least annually and after material changes to services, risks, or obligations. Publish approved revisions with an effective date. Meier Made does not claim independent security certification or guaranteed platform approval through publication of this policy.

Related policies

- Privacy Policy
- Data Deletion
- Security Reporting