

OmniTech Solutions

User Identity & Access Management Guide

Classification: Internal Use Only

Version: 5.2

Last Updated: October 2024

Section 1: Password Requirements

1.1 Minimum Security Standards

To ensure the security and integrity of customer data, all OmniTech accounts created after January 1, 2024 (Q1 2024 security update) must adhere to the following password complexity standards:

Requirement	Specification	Example
Minimum Length	8 characters (12+ strongly recommended)	SecureP@ss2024!
Uppercase Letters	At least one (A-Z)	P in 'Password'
Lowercase Letters	At least one (a-z)	a in 'Password'
Numeric Digit	At least one (0-9)	2024
Special Character	Recommended but not required	@ ! # \$ %
Username/Email	Cannot contain username or email address	USA

1.2 Prohibited Password Patterns

OmniTech's authentication system actively blocks commonly compromised passwords using the Have I Been Pwned database of over 800 million exposed credentials. Additionally, the following patterns are prohibited:

- Sequential characters: 'abc123', '12345678', 'qwerty'
- Repetitive characters: 'aaaaaaaa', 'password1111'
- Dictionary words: 'password', 'welcome', 'omnitech'
- Personal information: birthdates, phone numbers, addresses visible in your profile
- Previously used passwords: System maintains history of last 10 passwords

1.3 Password Expiration and Rotation

Consumer accounts do not have mandatory password expiration. However, business and enterprise accounts enrolled in OmniTech Business Services must rotate passwords every 90 days in compliance with corporate security policies. Users receive email reminders 14 days, 7 days, and 1 day before expiration.

Best Practice Recommendation: Change your password immediately if you suspect unauthorized access, receive a security alert from OmniTech, or if the same password is used on another service that experiences a data breach.

Section 2: Resetting Credentials

2.1 Self-Service Password Reset

Users locked out of their accounts can utilize the 'Forgot Password' link prominently displayed on the login portal at www.omnitech.example.com/login. The password reset process follows these steps:

Step 1	Navigate to the login page and click 'Forgot Password' below the password field
Step 2	Enter the email address registered to your OmniTech account
Step 3	Complete the CAPTCHA verification to prevent automated abuse
Step 4	Check your email inbox for a password reset message (arrives within 2-5 minutes)
Step 5	Click the secure token link in the email (expires in 15 minutes for security)
Step 6	Create a new password meeting all complexity requirements
Step 7	Confirm the new password and submit
Step 8	Log in immediately with your new credentials

2.2 Troubleshooting Email Delivery

If the password reset email does not appear in your inbox within 5 minutes, perform the following checks:

- 1.Check your Spam/Junk folder - email filters may incorrectly flag automated messages
- 2.Verify the email address entered matches your account registration exactly
- 3.Confirm your email service is not experiencing outages or delivery delays
- 4.Check email rules or filters that may be routing OmniTech messages to specific folders
- 5.Wait 10 minutes total before requesting another reset (multiple requests do not expedite delivery)

If problems persist after these steps, contact customer support at support@omnitech.example.com with your account email address. Our security team can manually verify your identity and initiate a password reset.

2.3 Single Sign-On (SSO) Accounts

Enterprise customers who access OmniTech through corporate Single Sign-On systems (Azure AD, Okta, Google Workspace) do not manage passwords directly through OmniTech. If you see a message stating 'This account uses SSO authentication,' your password must be reset through your company's identity provider, not through the OmniTech portal.

To identify your SSO provider: Check your company's IT documentation, look for the email domain in your login screen (e.g., 'Sign in with @yourcompany.com'), or contact your internal IT help desk. OmniTech support cannot reset SSO passwords as we do not have access to your corporate identity management systems.

Section 3: Multi-Factor Authentication (MFA)

3.1 MFA Enrollment

Multi-Factor Authentication adds an additional security layer beyond passwords. When enabled, users must provide a second verification factor when logging in from a new device or location. OmniTech supports the following MFA methods:

Method	Description	Setup Time
Authenticator App	Google Authenticator, Authy, Microsoft Authenticator	2-3 minutes
SMS Text Message	6-digit code sent to registered mobile number	1 minute
Email Code	Code sent to registered email address	1 minute
Hardware Token	YubiKey, Titan Security Key (Enterprise only)	5 minutes

To enable MFA: Log into your account, navigate to Settings > Security > Multi-Factor Authentication, and select your preferred method. Follow the on-screen instructions to complete enrollment.

3.2 Backup Codes

When enrolling in MFA, OmniTech generates 10 single-use backup codes. Store these codes securely (password manager, secure note app, or printed in a safe location). Each code can be used once if you lose access to your primary MFA device. After using a backup code, the remaining codes stay valid but the used code is permanently invalidated.

Section 4: Account Deletion & Data Privacy

4.1 GDPR and CCPA Compliance

Under the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), users have the right to request complete deletion of their account and all associated personal data. This process is permanent and irreversible.

Account deletion removes:

- Complete purchase history and order records
- Saved payment methods and billing addresses
- Shipping addresses and delivery preferences
- Product reviews and community forum posts
- Support tickets and communication history
- Warranty registrations and service records

4.2 Deletion Request Process

To request account deletion, email privacy@omnitech.example.com with the subject line 'Account Deletion Request.' For security purposes, you must verify your identity by providing two distinct data points from the following list:

- Last four digits of a payment method on file

- Recent order number (within past 6 months)
- Shipping address associated with the account
- Answer to your security question (if configured)
- Phone number registered to the account

OmniTech will process deletion requests within 30 days as required by law. You will receive confirmation via email when deletion is complete. Note that certain transaction records may be retained for 7 years to comply with tax and financial regulations, but these are stored in de-identified form without linkage to your personal profile.

Security & Privacy Support

Email: privacy@omnitech.example.com

Security Team: security@omnitech.example.com

Phone: 1-800-555-0197 (Mon-Fri 9AM-6PM EST)

Privacy Portal: www.omnitech.example.com/privacy