MACKTEZ · TRUST & SECURITY

Security Overview

How Macktez secures the systems its clients depend on. Our program is designed to align with NIST CSF, ISO 27001, and SOC 2 controls. Last updated July 2026.

OUR POSTURE

Macktez is a New York City IT consulting firm and managed service provider, founded in 1996. As an MSP we administer the identity, endpoints, servers, cloud, network, backup, and security that organizations rely on daily. The controls we recommend to clients are the controls we operate under ourselves. Recognized as JumpCloud's MSP Partner of the Year (Americas) for identity, device management, and zero-trust work.

FRAMEWORK ALIGNMENT

NIST CSF 2.0

National Institute of Standards and Technology. Organized around Govern, Identify, Protect, Detect, Respond, Recover. Voluntary — not a certification.

ISO/IEC 27001:2022

Controls mapped to the organizational, people, physical, and technological themes of an ISMS. We run the building blocks; not certified.

SOC 2 (AICPA)

Operated to Security, Availability, Processing Integrity, Confidentiality, Privacy. An attestation report, not a certification.

On certification: Macktez is not the subject of a SOC 2 attestation and is not ISO 27001 certified — our program is designed to align with these frameworks, not audited against them. A SOC 2 report is issued by a CPA firm and ISO 27001 certification by an accredited auditor; neither is self-declared. We are glad to complete a security questionnaire or share documentation under NDA — and we help clients get audit-ready.

CONTROLS

Privileged access to client systems

- Unique, named admin identities — no shared logins
- Phishing-resistant MFA on all admin access
- Least-privilege, role-based access
- Secrets in a managed vault (1Password)
- Access reviewed and revoked on role change

Identity & access management

- SSO + MFA across managed platforms
- Conditional access / device trust
- Joiner/mover/leaver workflows
- JumpCloud, Microsoft Entra, Okta

Endpoint security

- Centrally managed (JumpCloud, Intune)
- Full-disk encryption (FileVault, BitLocker)
- EDR and managed antivirus
- Automated patching, remote wipe

Data protection & encryption

- TLS 1.2+ in transit; encryption at rest
- Data minimization
- Client environments kept separated
- Secure disposal / certified e-waste

Network security

- Next-gen firewalls, segmentation
- Zero-trust / VPN admin access
- No open inbound management ports
- Documented, hardened configs

Email & phishing defense

- SPF, DKIM, DMARC enforced
- Advanced malware/link protection
- BEC / impersonation safeguards
- Phishing awareness training

Monitoring, logging & alerting

- Centralized logging
- Alerting on anomalous auth/admin actions
- Retention for investigation

Vulnerability & patch mgmt

- Timely OS/app patching
- Vulnerability scanning, risk-based fixes
- End-of-life tracking

Incident response

- Documented IR plan with roles
- Clear client-notification paths
- Post-incident review

Continuity, backup & DR

- 3-2-1 backups, encrypted off-site
- Verified restore testing
- Documented RTO/RPO

Vendor & subprocessor mgmt

- Platforms hold SOC 2 / ISO attestations
- Least-privilege integrations, reviewed

People & governance

- Background checks where permitted, NDAs
- Structured onboarding/offboarding
- Annual security-awareness training
- Written policies, periodic risk assessment

REPRESENTATIVE SUBPROCESSORS

Microsoft 365 & Azure	Productivity, email, cloud infrastructure
Google Workspace	Productivity and email
Amazon Web Services	Cloud infrastructure and storage
JumpCloud	Identity, SSO/MFA, device management
Microsoft Entra & Okta	Identity and access management
1Password	Credential and secrets management
NinjaOne	Remote monitoring and endpoint management
Freshservice	Service desk and ticketing