The ActiveITO Standard

The security controls every client gets from day one, mapped to CIS Controls v8 and NIST CSF 2.0.

Version **1.0** Last updated **At launch** Controls **11**

1. Summary

The Standard is the list of security controls ActiveITO puts in place for every client, at every size, with no premium tier. It covers what insurers and auditors ask about first: who can sign in, whether computers are watched and patched, whether backups restore, and whether staff can spot a phishing email. Each control produces evidence you can hand to an insurer, auditor or client. Your monthly report shows whether each one passed.

2. The controls

#	Area	What we do	How we check it	Reference
2.1	Identity and MFA	MFA on every user and admin account. Older sign-in methods that skip MFA are blocked.	Monthly export of MFA status per account	CIS 6.3, 6.4, 6.5 · NIST PR.AA-03
2.2	Endpoint detection and response	EDR on every computer and server, monitored 24/7, with the power to isolate a machine at any hour.	Coverage checked against the device list monthly	CIS 10.1, 13.1 · NIST DE.CM-09
2.3	Patching	Critical patches within 14 days, others within 30.	Patch status per device in the monthly report	CIS 7.3, 7.4 · NIST PR.PS-02
2.4	Backups	Microsoft 365 and server data backed up daily to immutable storage, with one copy off-site.	A test restore every quarter	CIS 11.2–11.5 · NIST PR.DS-11

#	Area	What we do	How we check it	Reference
2.5	Email security	Phishing and malware filtering. SPF, DKIM and DMARC at enforcement on every sending domain.	DNS check and DMARC report review monthly	CIS 9.5, 9.7 · NIST PR.PS
2.6	Disk encryption	Full-disk encryption on every laptop and desktop, with recovery keys in your own Microsoft 365 tenant.	Encryption status per device monthly	CIS 3.6 · NIST PR.DS-01
2.7	Firewall and network	A supported firewall at each site, current firmware, no admin interface open to the internet, guest Wi-Fi kept apart.	Config review and external scan quarterly	CIS 4.2, 12.2 · NIST PR.IR-01
2.8	Admin access	No admin rights on everyday accounts. Admin work uses separate accounts, and it's logged.	Admin group report monthly	CIS 5.4, 6.5 · NIST PR.AA-05
2.9	Security awareness training	Training for everyone at onboarding and every quarter, with simulated phishing.	Completion and phishing results per person	CIS 14.1 · NIST PR.AT-01
2.10	Documentation	Every system, account, licence and vendor written down. You have read access at all times.	Reviewed at each quarterly review	CIS 1.1, 2.1 · NIST ID.AM-01
2.11	Incident response plan	A written plan: who calls whom, when to call your insurer, and the first hour's steps.	A tabletop test with you once a year	CIS 17.1–17.4 · NIST RS.MA-01

3. How we check it

Each control is checked on the schedule above, and the result goes into your monthly report as passed, in progress or failed. A failed control stays on the report, with a fix date, until it

passes. So the Standard is checked on your systems twelve times a year.

4. What it doesn't cover

Not

A certification or an audit

It's aligned to CIS Controls v8 and NIST CSF 2.0, and no auditor has certified it.

Not

A penetration test

If your insurer or a client asks for one, we'll help you scope it with a testing firm.

Not

Legal advice

The industry pages say what each rule asks for; your counsel decides what applies to you.

Not

A promise of zero incidents

It makes one less likely and shortens recovery. The incident response plan covers the rest.

5. Change log

Version	Date	Change
1.0	At launch	First published version.

(480) 555-0100 Privacy Terms Accessibility © 2026 ActiveITO