TeamViewer

The remote IT security checklist

Investing in the right remote technology takes time. Our checklist covers the essentials for providing secure remote IT support. Tick off every item now.

Implement strict password rules

Define employee safety protocols with single sign-on (SSO).
With SSO, colleagues need just one password to log in securely.
This removes the hassle of creating (and forgetting) multiple, weak passwords.

Build up your verification layers

Prevent unauthorized access with multi-factor authentication (MFA).
Before you grant users access to accounts, devices, and systems,
ensure they provide multiple forms of identification.

Disable remote input

Keep your remote session secure and uninterrupted
by disabling remote input. Connect remotely, confident
that the supported end user won’t break your flow.

Stop onlookers seeing your screen

No secure remote support solution is complete without
black screen functionality. It allows you to set your
remote device’s screen to turn black as you access it.

Keep up your security standards

Bring your own certificate (BYOC) policies allow you to use
your digital certificates to secure cloud services and applications.
This means more control over security standards and compliance.

Grant, restrict, and revoke access (your way)

Conditional access, the rule-based feature, allows you to take actions
based on criteria like user credentials, location, time, and device,
significantly tightening remote security.

Be selective when granting access

With granular access controls, you get full control over who has access
to specific devices within your organization. Apply special permissions,
licenses, and policies to teams, individuals, and devices.

Want to provide secure IT support that’s even more supportive?

Learn more