Remote Work Policy

Step-by-Step Guide & Examples for IT Managers

Prepared by OpenVPN

How to Write a Remote Work Policy: Step-by-Step Guide & Examples

Step 1: Define the Purpose and Scope

The first step is clarifying why the policy exists and who it applies to. This establishes alignment from the beginning and avoids confusion later. A purpose statement connects the policy to business objectives like security, productivity, or employee satisfaction. Scope defines which employees or departments are eligible.

> Example: “This policy applies to all full-time employees who request to work remotely three or more days a week. Contractors and temporary staff are required to use on-site facilities unless explicitly approved.”

> Benefit: A clear purpose and scope prevent misunderstandings and ensure that IT managers know exactly which endpoints and users to secure.

Step 2: Identify Remote Work Requirements

Not every role is suited to remote work, especially when sensitive systems or in-person responsibilities are involved. Identifying requirements upfront avoids friction between employees and management. Consider job function, access to sensitive data, and security obligations.

> Example: “Customer-facing roles may be approved for hybrid arrangements, while finance and compliance functions must work within secure office environments unless additional safeguards are implemented.”

> Benefit: This prevents risky data exposure and gives IT managers a framework for deciding which roles require stronger access controls.

Step 3: Set Expectations: Work Schedule, Performance, and Communication

A remote policy should clearly define when employees are expected to be available, how performance will be measured, and which communication tools are mandatory. This reduces ambiguity and helps IT track approved collaboration platforms.

> Example: “Employees are expected to be available from 9 a.m.–5 p.m. EST, check in via Slack at least once daily, and submit weekly project updates in Asana.”

> Benefit: By setting these expectations, managers gain clarity on productivity, and IT managers ensure employees don’t turn to shadow IT tools that introduce security risks.

Step 4: Specify Equipment and Technology Needs

Employees need secure, reliable equipment to perform effectively. Standardizing devices and technology not only streamlines support but also enhances endpoint security.

> Example: “Company-issued laptops with OpenVPN Access Server pre-configured must be used for all work-related tasks. Personal devices are not permitted for accessing internal systems.”
>
> Benefit: IT managers maintain control over devices, enforce encryption, and reduce the likelihood of breaches caused by insecure personal hardware.

Step 5: Data Security and Privacy Protocols

Data security should be non-negotiable. Remote work policies must detail encryption requirements, approved VPNs, authentication methods, and secure file-sharing protocols.

> Example: “All employees must connect through OpenVPN CloudConnexa to access internal applications. MFA is required for all logins, and confidential data must be shared via approved platforms only.”
>
> Benefit: IT managers gain visibility into access points, reduce compliance risks, and safeguard sensitive business data.

Step 6: Establish the Approval Process

An approval process formalizes how employees request remote access and how IT validates their eligibility. This keeps access tightly controlled.

> Example: “Employees must submit a formal request through HR. Once approved, IT will provision secure access credentials through OpenVPN Access Server.”
>
> Benefit: IT managers enforce least-privilege access and maintain continuous monitoring, preventing unauthorized users from slipping through.

Step 7: Support Employee Health and Well-Being

Remote work isn’t just about laptops and VPNs—it’s about ensuring employees can thrive outside the office. Encouraging wellness promotes productivity and retention.

> Example: “Employees are encouraged to set up ergonomic home workstations. The company provides stipends for chairs and monitors. Breaks are required every 2 hours.”
>
> Benefit: Healthy, supported employees are more engaged, which reduces IT support tickets caused by burnout or disengagement-related errors.

Step 8: Expand on Training and Ongoing Support

Technology is only as strong as the people using it. Ongoing training ensures employees understand both the policy and the tools they must use.

> Example: “All employees must complete quarterly security awareness training, including simulated phishing exercises and OpenVPN usage best practices.”
>
> Benefit: IT managers can rest easier knowing the workforce is equipped to recognize threats and use company-approved systems correctly.

Step 9: Regular Policy Reviews and Updates

Remote work evolves quickly. A review cycle ensures policies stay relevant as technology, regulations, and business needs change.

> Example: “The HR and IT departments will review and update this policy every six months or following major compliance updates.”
>
> Benefit: This keeps IT managers ahead of emerging threats and reduces gaps that attackers could exploit.

Step 10: Detail Termination of Remote Work Arrangements

It’s just as important to define how and why remote privileges may end. Clear guidelines maintain accountability and protect the business.

> Example: “Remote access will be revoked if employees fail to meet security, compliance, or performance standards. Upon termination, IT will disable access credentials immediately.”
>
> Benefit: Ensures IT managers can swiftly de-provision access, reducing the risk of insider threats or data leaks.