VENDOR ACCESS / MSP / POLICY

Vendor Access Policy

A policy for controlling MSP, contractor, software vendor, and support-provider access to business systems.

Purpose

This policy explains how vendors, MSPs, contractors, consultants, and support providers may access company systems.

The goal is to ensure the company remains in control of its own infrastructure, accounts, credentials, documentation, and data.

Scope

This policy applies to any non-employee who accesses company systems, networks, applications, cloud tenants, data, devices, facilities, or administrative portals.

Covered vendors may include MSPs, software support vendors, phone providers, camera installers, network installers, cloud consultants, accounting software providers, web developers, and security consultants.

Access approval

Vendor access must be approved before access is granted. Approval should identify:

- Business reason for access
- Systems in scope
- Access level needed
- Named vendor users
- Start date
- Expected end date
- Company owner responsible for the vendor
- Whether remote access is required

Vendors should receive only the access needed to perform the approved work.

Named accounts

Vendors should use named accounts whenever possible. Shared vendor administrator accounts should be avoided because they make it difficult to know who performed an action.

If a shared account is unavoidable, the password must be stored securely, access must be limited, and the password must be rotated when vendor personnel change or the vendor relationship ends.

Administrative access

Administrative access must be limited to approved systems and approved time periods. Standing global administrator access should be avoided unless there is a documented business reason.

For high-risk systems, the company should use just-in-time access, temporary elevation, monitored sessions, or approval-based access where practical.

Remote access tools

Vendors may use only approved remote access tools. Consumer remote access tools, unattended agents, hidden access methods, personal VPNs, or vendor-controlled backdoors are not allowed without explicit approval.

The company should maintain an inventory of remote access agents and vendor portals.

MFA and authentication

Vendor accounts must use MFA where supported. Vendor access should not rely on passwords alone.

The company should not allow vendors to use one shared MFA method across multiple people. MFA methods should be tied to named users whenever possible.

Documentation and handoff

Vendors must provide documentation for systems they install, configure, or manage. Documentation should include:

- System purpose
- Administrative URLs
- Ownership and licensing details
- Configuration backups where appropriate
- Network diagrams or connection notes
- Support contacts
- Warranty or renewal information
- Credentials handoff process
- Known risks or limitations

The company should store this documentation in an approved company-controlled location.

Vendor offboarding

When a vendor relationship ends or access is no longer needed, the company must:

- Disable vendor accounts
- Revoke active sessions
- Rotate shared passwords
- Remove remote access agents
- Remove VPN access
- Remove vendor MFA methods
- Update recovery email addresses and phone numbers
- Transfer ownership of documentation, licenses, and portals
- Verify that DNS, domains, cloud tenants, firewalls, backups, cameras, and management systems are under company control

Emergency access

Emergency vendor access may be granted when needed to restore operations or protect safety. Emergency access should still be documented, time-limited, and reviewed afterward.

Review schedule

Vendor access should be reviewed at least quarterly for critical systems and at least annually for all vendors.

Implementation checklist

- Inventory vendor accounts
- Inventory remote access tools
- Require MFA for vendor access
- Remove old MSP accounts
- Store vendor documentation in a company-controlled location
- Track contract end dates and renewal dates
- Rotate shared credentials after vendor changes
- Keep domain, DNS, cloud tenant, and firewall ownership under company control

Disclaimer

This starter policy is general information, not legal advice. Adapt it to your business, contracts, regulatory obligations, and state law.