CYBERGLASS SECURITY STANDARDS

Remote Access Standard

Mandatory requirements for remote working and remote access to [Company Name] information, systems and networks, including devices, travel and third parties.

Organization	[Company Name]
Document ID	STD-02
Document owner	[Name, title]
Approved by	[Name, title]
Version	1.0 [draft / approved]
Effective date	[YYYY-MM-DD]
Next review	[YYYY-MM-DD] (at least every 12 months)
Classification	Internal

PREVIEW

About this template (delete this box before publishing)

This document is a template to help [Company Name] write its own policy. It is a guideline based on common industry practice and publicly available frameworks, not a finished policy, legal advice or a guarantee of compliance. Every organization is different: review each requirement, remove what does not apply, add what is missing, and set values your organization can actually meet. Have the final version reviewed by people who know your systems, obligations and risks.

- Replace every [bracketed] value with what your organization can actually achieve. Auditors test you against what you write.
- "Shall" means mandatory, "should" means expected unless a documented reason exists, and "may" means optional.
- Complete the approved methods table in section 5.2 with the remote access methods you actually use; anything not listed should be disabled.
- Choose your position on personal devices in section 5.3 before publishing: browser or virtual desktop only (recommended), or not permitted at all.
- Replace every highlighted **[placeholder]** with your organization's details, then remove the highlighting.
- Grey **Guidance** boxes explain what auditors, insurers and clients look for. Read them, then delete them before publishing.

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

1. Purpose

This Standard defines the security requirements for remote working and for remote access to [Company Name]'s information, systems and networks. Remote access technologies, such as virtual private networks (VPN), zero-trust network access, virtual desktops and cloud services, carry [Company Name] information over shared infrastructure such as the internet and extend the organization's boundary into homes, public places and third-party environments. Consistent controls are therefore required to keep these connections secure and to protect the confidentiality, integrity and availability of [Company Name] information.

This Standard is self-contained. It states [Company Name]'s remote access policy and the minimum controls against which compliance will be assessed.

2. Objectives

The objectives of this Standard are to ensure that:

a) remote access to [Company Name] information and systems is granted only to authorized individuals, for approved purposes, using approved access methods
b) every remote connection is strongly authenticated and encrypted
c) devices used for remote access meet defined security requirements before they are allowed to connect
d) remote working environments, including travel, are protected against loss, theft, eavesdropping and unauthorized disclosure
e) third-party remote access is controlled, attributable, time-limited and reviewed
f) remote access activity is monitored so that misuse and compromise are detected and acted upon promptly.

3. Scope and Application

This Standard applies to:

a) all employees, contractors, consultants, temporary staff and third parties ("users") who work remotely or access [Company Name] resources from outside [Company Name] premises
b) all service providers and vendors who connect remotely to support, maintain or monitor [Company Name] systems
c) all remote access technologies, including VPN, zero-trust network access, virtual desktop infrastructure, remote desktop gateways, cloud and software-as-a-service applications, and remote support tools
d) all devices used for remote access, whether owned by [Company Name], by users or by third parties
e) all new, emerging and existing technologies that provide remote access.

All systems and remote access arrangements are expected to meet this Standard. Where a requirement cannot be met because of technical limitations, end-of-life technology or a specific business need, a security risk assessment shall be performed and an exception requested in accordance with section 7.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop

4. Remote Access Policy

[Company Name] shall permit remote access only where:

a) it is required for an approved business purpose and authorized by an appropriate business representative
b) it is provided through a remote access method approved by [IT Security] (section 5.2)
c) the user is uniquely identified and authenticated with multi-factor authentication (MFA)
d) the connection is encrypted end to end using approved protocols
e) the connecting device meets the requirements of section 5.3
f) access is limited to the systems and information required, and is logged.

This Standard and any supporting procedures shall be:

a) approved by the [Chief Information Security Officer (CISO) or equivalent]
b) supported by periodic compliance reviews of remote access arrangements
c) reviewed at least annually and following significant changes to technology, threats or working practices.

5. Security Requirements

5.1 Remote working environments

[Company Name]'s remote working arrangements shall cover:

a) authorization by an appropriate business representative for an individual to work remotely, including the nature of the work permitted
b) the information security requirements that apply to remote working
c) physical protection of computing devices against loss and theft
d) secure methods for connecting to [Company Name] networks and services
e) requirements for individuals travelling outside [home country] with [Company Name] devices or information
f) the provision of technical support through the [IT Service Desk].

Remote working environments shall be protected by:

a) assessing risks specific to remote working, such as unknown physical security, shared households, home network equipment and collaboration platforms
b) providing remote access solutions, such as virtual desktops or browser-based access, that prevent [Company Name] information from being stored on unmanaged devices
c) restricting printing of confidential information at remote locations unless secure storage and disposal (for example lockable storage and cross-cut shredding) are available.

Individuals who work remotely shall:

a) be made aware of the additional risks of remote working, including theft of equipment, being overlooked or overheard, and accidental disclosure of information
b) be trained to perform the security tasks expected of them, such as locking devices, recognizing phishing and storing information only in approved locations
c) position screens and conduct calls so that confidential information cannot be seen or overheard by others, including household members
d) keep devices with them, out of sight or locked away when unattended, and never leave them in unattended vehicles
e) not allow family members, friends or other people to use [Company Name] devices or accounts
f) comply with applicable legal and regulatory requirements, including privacy and occupational health and safety obligations.

PREVIEW

Preview pages · full editable Word/Excel files at cyberglass.ai/shop