CYBERGLASS SECURITY STANDARDS

Access Management Standard

Mandatory requirements for identity, account, authentication and access rights management at [Company Name].

Organization	[Company Name]
Document ID	STD-01
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. Keep these words consistent when editing.
- Bracketed tools and platforms are examples only. Replace them with your own.
- Delete account types in section 7.1 that you don't use, but keep the generic account rows so their restrictions remain explicit.
- 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 establishes the mandatory requirements for managing identities, accounts and access rights to [Company Name]'s information systems, applications, services and data. It is a self-contained policy and standard: it states [Company Name]'s access control policy and defines the minimum controls against which compliance will be assessed.

2. Objectives

The objectives of this Standard are to:

a) ensure that access to information and systems is granted only to authorized entities for an approved business purpose
b) enforce the principles of least privilege, need to know and segregation of duties
c) provide individual accountability for all actions performed on [Company Name] systems
d) protect accounts against compromise through strong authentication
e) ensure that access rights are adjusted promptly when roles change and revoked promptly when no longer required
f) control and monitor privileged, generic, service and third-party access, which carry elevated risk
g) produce reliable evidence of access control effectiveness for management, auditors, clients and insurers.

3. Scope

This Standard applies to:

a) all [Company Name] business units, locations and subsidiaries, including remote and hybrid working arrangements
b) all employees, contractors, consultants, temporary staff, students, service providers and other third parties (collectively, "users") who access [Company Name] information or systems
c) all identities, whether human or non-human, including user, privileged, generic, service, application, API and device accounts
d) all information systems, applications, cloud services, directories, databases, endpoints and network and security devices owned, operated or contracted by [Company Name]
e) all environments, including production, disaster recovery, test and development where they contain [Company Name] or client data.

Physical access to premises is out of scope, except where physical access controls are integrated with logical identities. Any system that cannot comply with this Standard shall be managed through the exception process in section 10.

4. Access Control Policy

> **GUIDANCE** *(delete before publishing)*
> This section is the policy: the commitments senior leaders approve. The detailed requirements follow in sections 5 to 7.

PREVIEW

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

[Company Name] shall manage access to its information and systems through:

a) centralized identity and account management through an approved identity service ([central identity directory])
b) the use of approved third-party identity providers and federation only where governed by this Standard
c) the use of specialized access management capabilities where risk warrants, including single sign-on (SSO), multi-factor authentication (MFA) and privileged access management (PAM).

Access control at [Company Name] shall address:

a) the sensitivity of the information concerned, system owner requirements, and legal, regulatory and contractual obligations
b) access control rules and techniques, including role-based and attribute-based (conditional) access
c) the creation, amendment and deletion of accounts, and the allocation, modification, review and removal of access rights
d) authentication mechanisms, including passwords, passphrases, tokens, certificates, passkeys and biometrics
e) sign-on processes, including SSO and MFA
f) identity and access management solutions, including those integrated with cloud services and federated access.

This Standard and any supporting procedures shall be:

a) approved by the [Chief Information Security Officer (CISO) or equivalent]
b) supported by periodic review or audit of access control arrangements to confirm compliance
c) reviewed at least annually and updated following significant organizational, technological or regulatory change.

PREVIEW

5. Access Control Requirements

5.1 Access control implementation

Access control implementations shall ensure that:

a) accounts are created, modified and deleted only for defined entities, typically individuals and, where required, applications or services
b) each account, or group of accounts, is assigned rights to one or more specified systems, services or applications
c) access to [Company Name] resources is explicitly granted; access not expressly granted is denied by default
d) the permitted actions on each resource (for example read, create, update, delete, execute or approve) are defined, assigned, changed and removed in a controlled manner.

Access control implementations shall enforce:

a) access restrictions in line with the requirements set by owners of business applications and systems
b) restriction of access to only those networks, services and applications required
c) minimization of the number of accounts holding administrative or special privileges
d) visibility of who has access to which systems and information, and verification that access is used only for authorized purposes.

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