Cloud Security Template Toolkit

The OpenVPN Cloud Security Template Toolkit is designed to help organizations evaluate, strengthen, and standardize their cloud security posture as they adopt and manage modern, distributed environments. This toolkit includes four practical templates—the Cloud Security Checklist, an Access Control Policy Template, a SaaS Security Checklist, and the Buyers' Guide Vendor Checklist—each created to support clear decision-making, consistent governance, and risk-aware security practices. Together, these resources provide a structured starting point for assessing security readiness, defining access controls, evaluating SaaS usage, and selecting trusted vendors in the cloud.

Cloud Security Architecture Principles Checklist

Below are key principles for a rock-solid cloud security architecture, divided into four main categories: risk assessment and management, security framework development, compliance integration, and operational resilience.

Risk assessment and management	
☐ **Identification of users and assets**	Inventory cloud users, resources, associated roles, and access levels.
☐ **Business context, policies, and risk strategy**	Align cloud strategy with business context, policies, and risk thresholds.
☐ **Vulnerability and threat identification**	Continuously assess your cloud environment for known vulnerabilities and emerging threats.
☐ **User identity and access management**	Gain visibility and control over user authentication, roles, and privileges.
☐ **Activity monitoring**	Observe system behavior in real-time to detect anomalies, policy violations, and indicators of compromise.
Security framework development	
☐ **Security controls**	Implement guardrails to protect users, data, and infrastructure.
☐ **Configured responsibilities and security standards**	Define roles and expectations for managing security across services.
☐ **Data encryption**	Apply encryption protocols to protect all sensitive data at rest and in transit.

Compliance integration	
☐ **Data protection standards**	Ensure alignment with HIPAA, GDPR, and other regulatory frameworks.
☐ **Visibility across cloud deployments**	Maintain transparency across public, private, and hybrid clouds.
☐ **Regular verification**	Perform scheduled audits and security checks to validate adherence.
Operational resilience	
☐ **Monitor traffic in and out of the cloud**	Track ingress and egress points to detect anomalies.
☐ **Segment the architecture**	Isolate workloads to reduce the blast radius of an attack.
☐ **Automate cloud security tasks**	Use automation to enforce policies, remediate issues, and streamline workflows.
☐ **Ensure architecture flexibility**	Design with adaptability in mind for future needs and emerging threats.

Access Control Policy Template

Index

Objective and purpose

The purpose of this guide is to document rules for accessing [organization name]’s systems, applications, devices, resources, assets, data, and facilities. This guide will apply to all employees, contractors, and subcontractors of [organization name].

Access controls establish standards and procedures for preventing unauthorized access to information assets.

Access rights to [organization name] system components are limited to authorized personnel and are based on a user's role and responsibilities. Access rights to [organization name] system components must adhere to the concept of least privilege at all times.

Reference Documents

[Add links to your company's reference documents, if not listed below.]

- Information Security Policy
- Statement of Applicability
- [Information Classification Policy]
- [Statement of Acceptance of the ISMS Documents]
- [List of Legal, Regulatory, Contractual, and Other Requirements]

Controls

Least Privilege

The principle of least privilege grants users the bare minimum level of access to operating systems that is needed to perform their role or carry out their job responsibilities. [organization name] applies least privilege to its systems to add an additional layer of security over the data and information that a user handles and to reduce the risk of users abusing their access privileges.

Privileged Users

Privileged users are those with elevated or superuser access to in-scope systems and system components that are granted according to business needs. Privileged users (e.g., system administrators, IT engineers) are responsible for ensuring that the access rights for all users are commensurate with the following:

- The user's role and responsibilities within [organization name] (this principle is known as role-based access control).
- The concept of least privilege and separation of rights based on job duties.

Provisioning Users

When an employee or contractor joins [organization name], they are given the appropriate tools and access to [organization name] systems. During the process of onboarding, employees are assigned unique identifications (ID) and are sent the organization's policies. Employees must acknowledge having received and read the policies before being granted access to the information systems and networks needed to carry out their roles and responsibilities.

Users for all in-scope systems and system components are provisioned using all applicable provisioning and de-provisioning tools as necessary.

In-scope systems include the following:

- Organizational networks
- Applications
- Operating systems (OS)
- Data stores
- Cloud service provider (CSP) console
- Encryption keys
- Firewalls
- Log data

User Identifications

When a new user is onboarded, they are assigned a unique [organization name] employee ID. This ID defaults to the user's first name in lowercase text. If that ID already exists, then the ID will be the user's first and last name.

Employees are strictly prohibited from sharing IDs or from using another user's ID, regardless of whether the other user has granted permission.

User Access

Once an ID has been assigned to a new user, a formal access request ticket or email must be submitted to and approved by the appropriate system owner or a manager. When the access request is approved, the new user is given access to their [organization name] email, internal resources, and any other elevated permissions that their role requires them to have.

This same process is applied when existing employees require additional levels of access.

Deprovisioning Users

For any modifications to or removal of access, a formal access request ticket or email is required to ensure these actions are documented and completed in a timely manner. Terminated employees have access revoked within twenty-four (24) hours of termination.

Access Review Policy

All employee access to production systems is reviewed by management at least annually to confirm the access of each employee is appropriate and complies with the principles of least privilege and separation of duties.

The access review and any modifications to system access are formally documented and tracked.

Identification and Authentication Policy

[organization name] uses automated access control systems to restrict user access to its network and data. These automated access controls require users to authenticate before they may access any of the following:

- [organization name]'s network
- [organization name]'s source code
- [organization name]'s and its customer data
- Other restricted data

All users must use multi-factor authentication (MFA) to ensure that access to in-scope system components are protected at all times. MFA is met by incorporating two (2) of the three (3) methods of authentication listed below:

- **Something a user knows:** Generally includes passwords, passphrases, personal identification numbers (PINs), or some other type of knowledge that is known by a user.
- **Something a user has:** Generally includes some physical attribute provided to a user (e.g., access card, badge reader, key fob, dynamically generated unique identifier).
- **Something a user is:** Generally includes a unique physical attribute of the user, commonly known as biometrics. Devices that read a user's biometrics for authentication include, but are not limited to, the following:
  - Iris scanners
  - Palm scanners
  - Fingerprint readers
  - Facial recognition utilities
  - Voice recognition devices

The use of non-authenticated user IDs (i.e., IDs with no password or security token) or user IDs not associated with a single identified user is prohibited. Shared or group user IDs are never permitted for user-level access unless approved by authorized personnel.

Password Policy

Passwords are a critical component of information security. Passwords protect user accounts and must be configured according to [organization name]'s password policies. [organization name] requires users to create and use complex passwords.

Passwords must be safeguarded, and owners should not share them with other users. Passwords used by all users must meet or exceed all stated [organization name] policies for password complexity requirements.

Password Complexity

[organization name] requires that all passwords meet or exceed all of the following guidelines:

- Contain at least eight (8) alphanumeric characters, one of which must be a number.
- Contain both upper and lowercase letters.
- Contain at least one special character (e.g., $%^&*()_+|~-=\`[]:";'<>?,/).

A poorly constructed password is weak and may result in compromised systems and data; weak passwords are therefore prohibited. Weak passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, etc.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.

Permission Control List

Role Category

This guide outlines rules for access to systems, services and facilities, while the [Information Classification Policy] outlines rules for access to specific documents and records.

The following job titles have permissions according to Role Category 1:

[department name]

[job title 1]

[job title 2]

[Copy this section as necessary]

Role Category 1 has these permissions:

Name of system/application/network/asset	User Rights
System 1	Ex. read, write, delete, execute, view only, etc.

Rights Management

Rights (allowing or revoking access permissions) are conducted in the following way:

Name of system/application/network/asset	Name of authorized person(s) who can add or revoke access rights	Name of auditor	Date of periodic audit

The authorized person(s) must consider risk management for access. System owners and admins must perform routine audits to ensure that all system access rights are up to date. Periodic audits for terminated employees should be conducted.

SaaS Security Checklist

Component	Description
☐ **Multi-factor authentication (MFA)**	Verifies user identity by requiring an additional code or prompt in addition to a username and password.
☐ **Threat monitoring**	Tracks user activities in real-time to spot unusual behavior early and prevent potential breaches.
☐ **Regular access reviews**	Assesses who can view or change critical data, removing inactive or unauthorized users.
☐ **Network segmentation**	Divide your network into smaller zones to contain threats, minimizing damage if one segment is compromised.
☐ **Incident response plan**	Outlines a clear method to contain and resolve security incidents, with specific steps for different team members or departments.
☐ **Data encryption**	Protects data at rest and in transit using robust encryption standards, reducing the risk of exposure even if an attacker gains partial access.
☐ **Logging and audit trails**	Generates detailed records of user logins, configuration changes, and other key events, helping in compliance audits and forensic investigations.

Vendor checklist

Save this checklist for easy reference as you evaluate vendors and make notes on each vendor you're evaluating. Although each vendor may not check every box, you can use this sheet to prioritize your SMB's needs and compare vendors easily.

Note: this guide and checklist can be used to evaluate any security vendor and is not limited to network security providers.

- ☐ Pricing sheet available? _____
- ☐ Free trial or connections? _____
- ☐ List of recent security vulnerabilities / security compliance _____
- ☐ Integrations with current tech stack _____
- ☐ Existing customer reviews or references available _____
- ☐ Free technical support _____
- ☐ Scalability: Adding concurrent connections or future users _____
- ☐ Deployment: On-prem or cloud? _____
- ☐ Technology: Does the company roadmap reflect our future goals? How are the vendor's updates prioritized and implemented? _____
- ☐ Technical notes _____
- ☐ Additional Notes _____

_____

_____

_____

_____