Cloud Security Standard

*Revision:*

*Effective Date: ddmmyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Industry Configuration Standards 3

1.5 Related Documents / References 4

2. Standard Statements 5

2.1 GENERAL SECURITY CONTROLS AND PERMISSIONS 5

● SECURITY TEAM ACCESS AND PERMISSIONS 5

● NETWORK CONNECTIVITY 5

2.2 CLOUD NATIVE SECURITY CONTROLS 5

● AMAZON WEB SERVICE (AWS) ENVIRONMENTS 6

● MICROSOFT AZURE ENVIRONMENTS 7

● GOOGLE CLOUD PLATFORM (GCP) ENVIRONMENTS 10

3. Standard Compliance & Enforcement 12

3.1 Compliance Measures 12

3.2 Enforcement 12

4. Exception Process / Glossary 13

4.1 Exception Process 13

4.2 Glossary / Acronyms 13

5. Document Management 14

5.1 Document Revision Log 14

5.2 Document Ownership 14

5.3 Document Coordinator 14

5.4 Document Approvers 14

5.5 Distribution 14

# Introduction

## Document Definition

This document is a Standard.

For a full description of document types, see XXXX-POL-ALL-001 - Information Security Policy Framework.

## Objective

The purpose of this document is to define mandatory requirements, configuration best practices

(BPA) and security standards for services and environments hosted on public cloud environments. XXXX’s current cloud providers are listed below, but this Standard shall be applied to any public cloud that will be used for hosting XXXX information and/ or systems in the future.

## Scope

### Applicability to employees

XXXX refers to XXXXas well as its majority-owned subsidiaries and joint ventures (if applicable). This Standard applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Standard statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Standard applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Industry Configuration Standards

* [https://docs.microsoft.com/en](https://docs.microsoft.com/en-us/azure/architecture/framework/" \l "security)[-us/azure/architecture/framework/#security](https://docs.microsoft.com/en-us/azure/architecture/framework/#security)
* <https://docs.microsoft.com/en-us/azure/role-based-access-control/transfer-subscription>
* [https://docs.microsoft.com/en-us/azure/security/fundamentals/paas-applications-using-sql#benefits-ofusing-azure-ad-instead-of-sql-authentication](https://docs.microsoft.com/en-us/azure/security/fundamentals/paas-applications-using-sql#benefits-of-using-azure-ad-instead-of-sql-authentication)
* [https://docs.microsoft.com/en-us/azure/security/fundamentals/paas-applications-using-appservices#authenticate-through-azure-active-directory-ad](https://docs.microsoft.com/en-us/azure/security/fundamentals/paas-applications-using-app-services#authenticate-through-azure-active-directory-ad)
* [https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managedidentity-best-practice-recommendations](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identity-best-practice-recommendations)

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema>

<https://docs.microsoft.com/en-us/azure/azure-monitor/monitor-reference>

<https://docs.microsoft.com/en-us/powershell/module/az.sql/set-azsqldatabaseaudit?view=azps-6.4.0>

[https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-actiongroups-and-actions?view=sql-server-2017#database-level-audit-actions](https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-2017#database-level-audit-actions)

<https://cloud.google.com/architecture/framework/security>

<https://cloud.google.com/security/best-practices>

<https://cloud.google.com/compute/docs/instances/preventing-accidental-vm-deletion>

* <https://cloud.google.com/resource-manager/docs/project-liens>

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Standard Statements

## GENERAL SECURITY CONTROLS AND PERMISSIONS

## SECURITY TEAM ACCESS AND PERMISSIONS

Security teams require access to cloud environments in order to audit, monitor, and effectively respond to emerging threats. The security team shall be assigned permissions on a top-level administrative hierarchy, if applicable (e.g. GCP Organization, Azure Root Management Group, AWS Organization). The required permissions for each team are as follows:

**SOC team:**

* Read-only access to review the configuration of resources and conduct analysis of security incidents.

**Cloud Security Team:**

* Read-only access to review the configuration of resources and conduct in-depth investigation and analysis of security incidents.
* Limited access to manage specific cloud security services (Amazon GuardDuty, AWS Config, Microsoft Defender for Cloud, GCP Security Center Admin, Logging Admin, etc.).
* Additional permissions, if required, to assess the security impact of configurations, manage policies, and automate account security compliance with the company’s security policies.

Access to team ticketing systems to communicate with them on any security issues within their environments.

## NETWORK CONNECTIVITY

* By default, all services shall be assigned the least privileged network access.
* Each VPC/ VNET shall have a unique IP address space aligned within XXXX’s network environments and registered by the relevant network team.
* Default VPCs shall be avoided.
* Any exceptions to this requirement shall be formally agreed in writing with the Cloud Security Team using the Exceptions request form.

## CLOUD NATIVE SECURITY CONTROLS

The following settings shall be in place for each cloud environment managed by XXXX:

## AMAZON WEB SERVICE (AWS) ENVIRONMENTS

* AWS environments shall follow design best practices as defined by XXXX’s policies and procedures.

AWS Well-Architected Framework Security Pillars, and widely followed international security standards including CIS, NIST, ISO 27001, and others should be followed if relevant.

**Best practice for**

**AWS environments**

**:**

▪



* Public facing services such as S3 buckets, SQS or some API-level management calls shall have their source IP addresses whitelisted to the service’s ranges as defined in the identity or resource access policy.

**AWS Organization**

* AWS accounts shall be created under the XXXX AWS Organization. Any existing accounts owned by XXXX sitting outside the Organization shall be added into the XXXX AWS Organization. Account owners shall provide the account ID and root email to the Cloud FinOps Team who will invite the account to the Organization.
* XXXX AWS accounts are created by the Cloud FinOps team. Employees shall not create an AWS account by themselves.
* The billing configuration for each AWS account is provided by the Cloud FinOps team and is out of scope for this standard.
* Cloud service managers or BU leads shall notify the cloud security team in case of the creation, decommission, or major changes to the AWS account environment (including promotion to production, new processing activity on special type data such as personal, confidential or highly sensitive data, or the deployment of new applications or services).

**Root email**

* AWS account roots shall be registered to a XXXX corporate email address.
* The root account email shall not be owned by a single person. Root account email addresses shall be assigned to a distribution list with between two and four people.

**Root credentials**

* Root account usage shall be strictly limited to situations requiring this level of permission only.
* MFA shall be configured for the root account user and no Access Keys shall exist.
* Root account credentials shall be kept by the Account owners and, if required, shared with a very limited number of employees within the relevant team.

**AWS IAM**

* Customer-managed IAM and resource policies shall follow the ‘least privilege’ principle.
* Credential lifespans shall be limited by assigning relevant roles to EC2 instances and services according to AWS recommendations and architecting a credentials rotation policy for applications.
* All credentials shall be stored in an encrypted form according to **SEC-POL-10 Cryptographic Usage Policy**.
* MFA is required for all user accounts in addition to passwords.

**Best practice for AWS IAM:**

▪

The

existing XXXX Azure Active Directory

and/or

INFRA

LDAP

can be used

as

an identity source

in

AWS.



**Alternate security contact**

* An additional security contact shall be added to each account. The email address for the security contact is: soc@XXXX.com.

**AWS CloudTrail**

* AWS CloudTrail shall be enabled for all regions within the AWS account and stored in the S3 bucket managed by the Cloud Security team. It is prohibited to disable CloudTrail.
* Read/Write and KMS events shall be logged, and validation of log files shall be enabled.

**Best practice for AWS CloudTrail:**

▪

Logging of data events like S3 and Lambda

sh

ould

be configured

if needed

.



**Amazon GuardDuty**

* Amazon GuardDuty shall be enabled for all regions within the AWS account to report to the Master account managed by the Cloud Security team. It’s prohibited to disable the GuardDuty service.

**AWS Config**

* The AWS Config service shall be enabled in each active region to send logs to the Security S3 bucket.

## MICROSOFT AZURE ENVIRONMENTS

* Microsoft Azure environments shall follow design best practices as defined by XXXX policies and procedures, Microsoft Azure Well-Architected Framework Security pillars[[1]](#footnote-1), and widely followed international security standards including CIS, NIST, ISO 27001, and others as relevant.
* RDS services (Azure SQL, Azure PostgreSQL, and Azure Cosmos DB) shall not be publicly accessible.
* Additional measures to prevent unintended deletion of resources shall be implemented (e.g. Locks on the Resource Group, or use of the “delete” Lock on the Resource itself).
* The name of the subscription shall be descriptive (i.e. contain the project name). Default names like “Azure subscription 1”, “Azure testing subscription”, etc., shall not be used.
* Subscriptions created by the Visual Studio Subscription Portal, shall not be renamed, and shall not contain Production workloads or PII data unless details are agreed upon and approved in written form by the Cloud Security team.

**Azure subscriptions**

* Azure subscriptions shall be created under the XXXX Root Management Group. Any existing subscription owned by XXXX sitting outside the Management Group shall be added into the XXXX Root Management Group. It shall follow the onboarding process as defined by the Cloud FinOps team. The technical implementation of the migration process is described in Microsoft’s documentation[[2]](#footnote-2).
* The Creation and decommission of Azure subscriptions in XXXX is managed by the Cloud FinOps team.
* Employees shall not create an Azure subscription by themselves (except those created via the Visual Studio portal).
* The billing configuration for each Azure subscription is provided by the Cloud FinOps team and is out of the scope of this standard.

* All accounts with owner permissions shall have MFA enabled.

**Best practice for Azure subscriptions:**

▪

For availability, owner permissions of the subscription

should

be granted to

several

users



**IAM**

* Specially created separate accounts shall be used for privileged access to the subscription,

(as required in **SEC-POL-9 Access Control Policy Clause 5.4**). MFA shall be enabled for these accounts.

* Custom IAM roles will follow the ‘least privilege’ principle.
* All credentials shall be stored in encrypted form according to **SEC-POL-10 Cryptographic Usage Policy**.
* XXXX’s Azure AD shall be used as an identity source for SQL DB4, Applications5, etc.

with secret rotation enabled.

**Best practice for IAM:**

▪

Secrets (passwords, keys, certificates)

should

be stored in the Azure Key Vault



* Managed identities are recommended6 to be used as an alternative way of authentication for applications.

**Microsoft Defender for Cloud**

Microsoft Defender for Cloud (formerly known as Azure Security Center) is a service enabled by default for each subscription. Defender for Cloud’s ‘Basic’ tier functionality provides overall monitoring capabilities for resources in the subscription and their configurations.

* Azure Defender shall be enabled for Azure subscriptions with production resources like SQL DB (not a managed instance), App services, Kubernetes, and Container Registries.

**Security contact**

High severity Microsoft Defender for Cloud alerts shall be sent to the subscription’s owner with SOC team copied in.

**Logging**

* Activity logs for events related to the subscription activity shall be sent to a separate storage (Security’s Log Analytics Workspace and optionally destined to the Event Hub and sent to the SIEM). Categories[[3]](#footnote-3), that shall be logged are as follows:
  + Administrative
  + Service Health
  + Security
* Resource logs (Key Vault, Firewall, AppGW, LB, etc.[[4]](#footnote-4)) shall be enabled and sent to the separate storage within the subscription.
* Azure AD audit logs shall be enabled and sent to separate storage and SIEM.

**Best practice for IAM:**

* SQL DBs logs should be configured on the database level[[5]](#footnote-5). Groups of audit logs[[6]](#footnote-6) should be discussed with each team separately, based on data sensitivity and the possible amount of generated logs.



## GOOGLE CLOUD PLATFORM (GCP) ENVIRONMENTS

* Google Cloud best practices shall be applied based on XXXX policies and procedures, the Google Cloud Architecture Framework: Security, privacy, and compliance[[7]](#footnote-7), the Google Cloud security best practices center[[8]](#footnote-8), and widely followed international security standards including CIS, NIST, ISO 27001, and others as relevant.
* Services containing data (Cloud Storage, BigQuery, Cloud SQL, Cloud Spanner, Cloud Pub/Sub, etc.) must not be publicly accessible.
* Deletion protection[[9]](#footnote-9) for VMs, or a lien placed on a project[[10]](#footnote-10) shall be applied to prevent the unintended deletion of resources.
* The name of the project shall be set on project creation and be descriptive (i.e. include the project name). Default random names shall be changed on project creation.

**GCP Organization**

* GCP projects shall be created under the XXXX GCP Organization. Any existing project owned by XXXX sitting outside the Organization shall be added into the XXXX GCP Organization, it shall follow the onboarding process as defined by the Cloud FinOps team.

The project owner shall provide the project ID to the Cloud FinOps team to be invited into the Organization.

* The creation and decommission of GCP projects in XXXX are managed by the Cloud FinOps team. Employees shall not create GCP projects by themselves.
* The billing configuration for each GCP project is provided by the Cloud FinOps team and is out of the scope of this standard.
* Cloud service managers or BU leads shall notify the cloud security team of the creation, decommission, or major changes to the GCP project environment (including promotion to production, new processing activity on special type data such as personal, confidential or highly sensitive data, or the deployment of new applications or services).

**IAM**

* MFA shall be enabled for all user accounts accessing the GCP Organization.
* Permissions for all accounts in the GCP Organization shall follow the ‘least privilege’ principle.
* Workload identity federation shall be used to grant access to GCP resources from onpremises or other cloud environments instead of using a service account key.
* All credentials shall be stored in an encrypted form according to **XXXX-POL-ALL-016 - Encryption & Key Management Policy**

Secrets (passwords, keys, certificates) should be stored in Cloud Key Management with rotation of secrets enabled.

**Best practice for IAM:**

▪



* Service accounts shall be used as an alternative way of authentication for applications.

**Essential contacts for security**

* Essential contacts for the “Security” category shall include the SOC email address.

**Logging**

* GCP project Audit Logs shall be sent to the SIEM via Pub/Sub in the Security project or any other compatible way. This shall be configured at the GCP Organization level.
* **MITIGATIONS**

In case of a security vulnerability or misconfiguration in the cloud environment, remediation of the findings shall be performed based on severity according to **XXXX-POL-ALL-012 - Incident Response Policy**

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Regular user access reviews | * Report of exited users removed from the cloud service |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Glossary / Acronyms

|  |  |
| --- | --- |
|  |  |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Distribution

1. [↑](#footnote-ref-1)
2. <https://docs.microsoft.com/en-us/azure/role-based-access-control/transfer-subscription> [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. [↑](#footnote-ref-4)
5. [↑](#footnote-ref-5)
6. [↑](#footnote-ref-6)
7. [↑](#footnote-ref-7)
8. [↑](#footnote-ref-8)
9. [↑](#footnote-ref-9)
10. [↑](#footnote-ref-10)