EPAM Cloud

SECURITY POLICY

EPM-CSUP – EPAM Cloud Service

Related Artifacts	
Ref.	**Name**
https://epa.ms/cloud-doc-terms	EPAM Cloud Terms and Conditions

Terms and Definitions	
EPAM Cloud Service (EPAM Cloud, Cloud)	A part of the existing EPAM ecosystem providing the possibility for project teams to manage virtual infrastructures in EPAM private regions and on external Cloud platforms via a self-service solution, as well as to monitor infrastructure performance and events, collect logs, process Cloud-related billing, etc.
EPAM Orchestration	A complex application enabling EPAM Cloud Service performance.
Cloud Asset (Asset)	Any value, hosted in Cloud. This includes, but is not limited to, information, virtual servers, hardware servers.
Cloud Security (Security)	A set of techniques, rules and regulations, aimed to protect assets within EPAM Cloud.
Security issue	Conditions under which vulnerabilities can arise.
Security check	Measures and steps taken to detect security issues and vulnerabilities.
Project	A Project in terms of EPAM Systems organizational chart.
Cloud UI	A Web application designed to provide access to EPAM Cloud facilities.
Maestro Command Line (Maestro CLI)	Command line interface designed to provide access to EPAM Cloud facilities.
External user	EPAM Cloud service user who is not employed by EPAM Systems.
Cloud user (user)	An EPAM employee using EPAM Cloud service.
Cloud action (action)	An action aimed to modify a virtual infrastructure in Cloud.
Primary contacts	Project Manager, Delivery Manager
Secondary contact	Project Coordinator
VM Owner	The user acting as a contact point for an instance and responsible for the instance security.

CONTENTS

1 INTRODUCTION 4
1.1 THE SCOPE OF THE DOCUMENT 4
1.2 PURPOSE OF THE DOCUMENT 4
2 PARTIES DEFINITION 4
3 EPAM CLOUD SECURITY RULES AND REGULATIONS 5
3.1 MAIN POINTS 5
3.2 ACCESS TO EPAM CLOUD 5
3.2.1 General Points 5
3.2.2 Permissions 6
3.2.3 Access to VMs 6
3.2.4 Service Accounts 7
3.2.5 Simple User Account 8
3.2.6 Providing Access to External Users 8
3.2.7 Project Deactivation 8
3.3 VMS MANIPULATIONS, APPLICATIONS, AND DATA 8
3.4 NETWORK SECURITY 9
3.5 EVENTS AUDIT 10
3.6 USING EXTERNAL CLOUD PROVIDERS 10
3.6.1 Security in AWS 10
3.6.2 Security in Azure 12
3.6.3 Security in GCP 13
3.7 VULNERABILITIES DETECTION AND MANAGEMENT 14
3.7.1 Security checks 14
3.7.2 Vulnerabilities management 15
3.8 CLOUD E-MAILS AND NOTIFICATIONS 15

1 INTRODUCTION

1.1 THE SCOPE OF THE DOCUMENT

The document describes the main concepts of security in EPAM Cloud Service, specifies the main approaches, rules and regulations applied to ensure the security of Cloud assets. It applies to all Employees of EPAM Systems and related contractors or third party users (if any).

The owner and approver of this document is the Head of Global IT Operations. EPAM Cloud Consulting team is responsible for its maintenance.

1.2 PURPOSE OF THE DOCUMENT

The purpose of the document is to define the main security-related approaches in Cloud and the scopes of responsibility of all parties.

2 PARTIES DEFINITION

2.1. Cloud Users (Users): EPAM employees using EPAM Cloud facilities for project or personal needs. A person becomes a Cloud User as soon as at least one project they are assigned to is activated in Cloud.

2.2. Security Department - a department responsible for the assets, technical and operations security in organization. Includes the following teams:

- 2.2.1. IT Security Team;
- 2.2.2. IT Security Infrastructure Team;
- 2.2.3. Security Operations Center (SOC);
- 2.2.4. Continuous Vulnerability Management Team (CVM).

2.3. Support Teams: all teams responsible for EPAM Cloud provisioning and maintenance.

2.4. Level 1 Support Team: EPAM Cloud team, responsible for Cloud infrastructure monitoring, escalation of complex issues to L2 Support Team, 24/7/365 availability, monitoring Cloud configuration and templates development, and other.

2.5. Level 2 Support Team: EPAM Cloud team, responsible for the development hardware servers, HP OO stack, HP CSA, OpenStack and their maintenance and development.

2.6. Level 2 Hybrid Cloud Support Team: EPAM Cloud team, responsible for maintenance and support of core EPAM Cloud services and infrastructure of EPAM Hybrid Cloud, security groups and user management.

2.7. Level 3 Support Team: EPAM Cloud team, responsible for fixing issues in the following areas: UI usability, UPSA integration, ESP Integration, reporting and billing, product issues, template libraries.

2.8. Cloud Consulting Team: EPAM Cloud team, responsible for initial project onboarding, existing project migration, migration process help, providing answers for general and specific Cloud Computing questions, client communication on architecture, delivery of training materials, EPAM Cloud knowledge base development, acknowledging user feedback, reacting on and monitoring initial user requests.

The team, responsible for EPAM Cloud policies review.

2.9. License Group: the team of EPAM employees, responsible for licensing and licenses verification in EPAM.

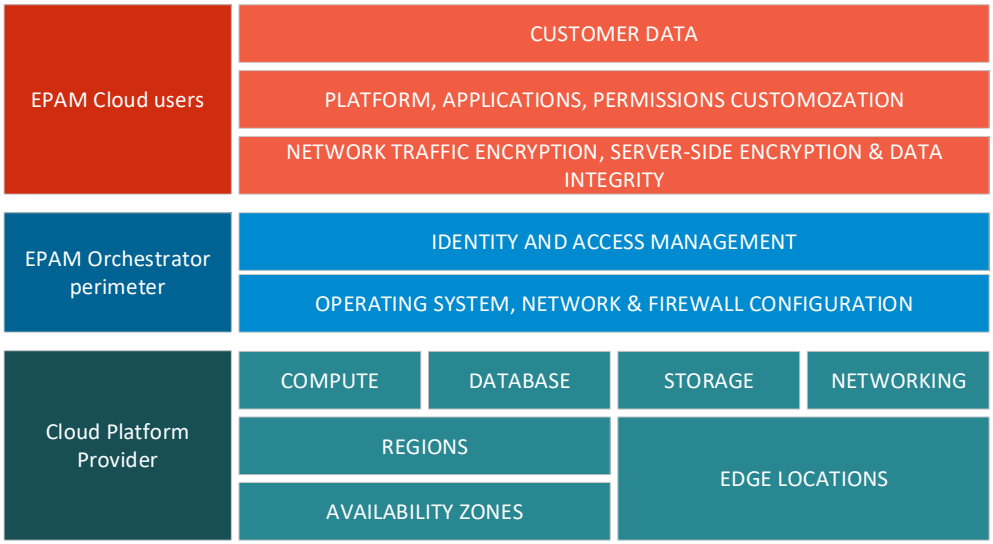
2.10. Network Team: the team of EPAM employees, responsible for networking settings and related operations.

3 EPAM CLOUD SECURITY RULES AND REGULATIONS

3.1 MAIN POINTS

3.3.1. EPAM Cloud follows the industry standard shared responsibility model, with additional layer covered by EPAM Cloud Orchestrator.

The general concept is given on the picture below:



3.3.2. EPAM Cloud is subject to the security policies applied in EPAM Systems, as well as to service-specific security rules and tools.

3.3.3. EPAM Orchestration update is performed according to the Production Update Plan, created by EPAM Cloud Support L3 team.

3.3.4. EPAM Cloud Support teams notify users on upcoming service unavailability by delivering respective SINs (Service Interruption Notifications) beforehand.

3.3.5. If necessary, the user should take all the measures that would ensure the security of their Cloud assets after the SIN period.

3.3.6. The user can utilize EPAM Orchestration's auto-configuration facilities to configure their infrastructures. Both out-of-the-box and custom scripts can be used for this purpose.

3.2 ACCESS TO EPAM CLOUD

3.2.1 General Points

3.2.1.1. The access to EPAM Cloud is provided on the domain level (with ADFS).

3.2.1.2. A user can access and manage the infrastructure only on the projects they are assigned to.

3.2.1.3. User's access to EPAM Cloud facilities is possible only after the activation of the respective project in Cloud. The activation is performed by request and after the approval of the project's manager or coordinator. The projects are charged for Service usage.

3.2.1.4. User access to EPAM Cloud is provided via Cloud UI and Maestro CLI.

3.2.1.5. Cloud UI application has two endpoints: the public one (https://cloud.epam.com), and the private one (https://console.cloud.epam.com).

3.2.1.6. The public endpoint of the Cloud UI is available via Internet and contains the library of documents describing EPAM Cloud solution.

3.2.1.7. The private endpoint of the Cloud UI is designed for virtual infrastructures management and monitoring, and is subject to Luminate SDP control, based on standard EPAM security policies, created and implemented by the Security Department.

3.2.1.8. Maestro CLI is available for download at Cloud Management Console within private endpoint.

3.2.1.9. The access via Cloud UI is provided via EPAM SSO tool and is possible from both EPAM network and Internet.

3.2.1.10. The access via Maestro CLI is available only from within EPAM network.

3.2.1.11. The access via Maestro CLI is provided by a unique UID, created by EPAM Orchestrator based on the user's EPAM domain or PMC credentials, and stored into a special (default.cr) file and in Orchestration's database.

3.2.1.12. Each user is responsible for the safekeeping of their default.cr file. The file directory must not be shared for external access.

3.2.1.13. The UID generated by EPAM Orchestrator should be changed by user each 3 months. Otherwise, the UID gets expired and the user cannot access Orchestrator with this UID, until it is updated.

3.2.1.14. Maestro Command Line allows up to 5 login attempts. If the user makes 5 consecutive failed login attempts, they get blocked in Orchestration for 30 minutes. The lock is removed automatically 30 minutes after the first incorrect credentials input. Unlocking by request is impossible.

3.2.1.15. The user can perform operations, allowed by EPAM Cloud hybridization with external cloud providers, via Cloud UI, Maestro CLI, and native tools of the respective provider.

3.2.1.16. EPAM Cloud functions can be accessed by external users (the users who are not employees of EPAM) only in exceptional cases, by request and after specific approval from EPAM Global Information Security Head and the responsible Account manager.

3.2.1.17. Each EPAM Cloud user should keep to standard EPAM AD credentials rotation policy.

3.2.2 Permissions

3.2.2.1. The scope of actions available for each user in Cloud is defined by their permission settings.

3.2.2.2. The default set of permissions for each user depends on their project role, according to the map described on User Permissions page/Account Management guide.

3.2.2.3. Project Manager, Project Coordinator, and Delivery Manager can customize permissions for specific users or role-based user groups by means of Cloud UI.

3.2.2.4. Project Manager, Project Coordinator, and Delivery Manager can delegate permissions to configure their project account in EPAM Cloud (both private and public clouds subscriptions) with the Manage Cloud wizard, available on the Cloud Dashboard.

3.2.3 Access to VMs

3.2.3.1. Access to VMs in EPAM Regions is performed via RDP with Domain credentials (for Windows), via SSH (for Linux), or VNC Client (for Mac).

3.2.3.2. If a VM is created within the scope of a platform service provisioning, the access credentials

can be generated by Orchestrator.

3.2.3.3. In case a user requests a hardware Mac server, they must change the default login credentials before they start working on this server.

3.2.3.4. If a VM access needs an SSH key, the public part can be stored in Orchestrator or at https://password.epam.com/

3.2.3.5. In case the SSH key used to login to a VM is stored on Orchestrator side, access to Linux-based VMs in any supported cloud is performed with the key and the user name depending on the operating system:

Image	Username
CentOS-based	centos
Debian-based	admin (private, AWS, Google) debian (Azure)
Ubuntu-based	ubuntu
CoreOS-based	core
Amazon Linux	ec2-user
Oracle Linux-based	oracle

3.2.3.6. VMs with Linux-based OS have a default technical account.

3.2.3.7. The default technical account can be used by Cloud Support and Security teams to access the VMs in case of emergency (serious security issues, issues affecting the performance of specific teams, projects, etc.), with prior notification of the upcoming activities.

3.2.3.8. The default technical account should not be updated or removed by project teams.

3.2.3.9. The user who updates or removes the default technical account is fully responsible for the consequences of this action, and can face disciplinary and administrative measures.

3.2.3.10. In case the SSH key used to login to a VM is stored at https://password.epam.com/, access to Linux VMs is performed with the key and the domain user name.

3.2.3.11. Access to Windows VMs in AWS is provided by decrypted AWS password.

3.2.3.12. Access to VMs in Azure is provided by credentials generated automatically at VMs creation. The credentials are not stored on Orchestrator's side.

3.2.3.13. Access to Windows VMs on GCP is performed under the Administrator user name, and the password, retrieved with the or2console command call (which should include an SSH key of 2048 size).

3.2.4 Service Accounts

3.2.4.1. A service account can be created by request to the Cloud Support team in order to facilitate CI/CD processes on the project.

3.2.4.2. A service account name should comply with the following syntax:
auto_<project_name>_<comment>@epam.com

3.2.4.3. A service account can access Maestro CLI and API.

3.2.4.4. The access is provided to a service account by a unique UID, created by EPAM Orchestrator based on the account's credentials, and stored into a special (default.cr) file and in Orchestration's database.

3.2.4.5. The UID generated by EPAM Orchestrator should be changed by the account owner each 12 months. Otherwise, the UID gets expired and the user cannot access Orchestrator with this UID, until it is updated.

3.2.5 Simple User Account

3.2.5.1. A simple user account is an account created manually by request to the Cloud Support team.

3.2.5.2. A simple user account is linked to a specific project.

3.2.5.3. A simple user account is created based on the existing EPAM service account, or for an external user, who needs to have access to EPAM Cloud.

3.2.5.4. A simple user account creation should be approved by the Project Manager.

3.2.5.5. A simple user account has limited access to EPAM Cloud, and the set of the provided permissions is based on the details of the user creation request.

3.2.5.6. A simple user account expires in 12 months after creation.

3.2.6 Providing Access to External Users

3.2.6.1. An external user can get access to viewing and managing virtual infrastructures of a project only by request from the project authorities (Project manager, Account Manager, Project Coordinator, Delivery Manager).

3.2.6.2. The external user permissions are defined by the user requestor, who should specify the list of permission groups to which the user should be assigned.

3.2.6.3. Each external user should be added to EPAM AD and assigned to the target project by project authorities before access to EPAM Cloud is granted to such user.

3.2.6.4. The external user account expires in 12 months after creation.

3.2.6.5. External users by default have no access to native management consoles of public cloud providers.

3.2.7 Project Deactivation

3.2.7.1. A project can be deactivated in Cloud by special request to the Cloud Support team.

3.2.7.2. All the project virtual resources should be terminated or migrated before the project is deactivated in Cloud.

3.2.7.3. When a project status is set to CLOSED in UPSA, the project is automatically deactivated in Cloud.

3.2.7.4. In case a project has virtual resources at the moment when the project closure request is submitted, the Cloud Support team contacts the project responsible persons to clarify whether the resources should be terminated or migrated, and acts according to the provided decision.

3.3 VMS MANIPULATIONS, APPLICATIONS, AND DATA

3.3.1. The applications, data, and settings included to default Cloud images, are verified by Enterprise admins and Security Department according to corporate security policy.

3.3.2. VM owner, Project Manager, Project Coordinator, and Delivery Manager are responsible for the securing and safekeeping of the data stored in project virtual infrastructure.

3.3.3. The user is responsible for all changes and customizations on the VMs under EPAM Orchestrator's control, unless this changes are applied by Cloud Support Team or Security Department.

3.3.4. The applications and data added to VMs by the user, as well as used via VMs, must comply with corporate licensing and security standards.

3.3.5. Each VM should have antimalware software installed. This software should be included to approved antimalware list (https://kb.epam.com/display/EPMITSVCFAQ/List+of+Recommended+Anti+malware+Software)

3.3.6. It is recommended to upload logs from VMs to an external log collector.

3.3.7. License-related rights and permissions are controlled by the License Group.

3.3.8. A custom image can be imported to EPAM Orchestration for a specific project, by request to EPAM Support Portal. Before the image is imported, it is subjected to security check by the License Group, Continues Vulnerability Management team (CVM), IT Security team. The import procedure is held by the Cloud Support team.

3.3.9. VMs and other virtual resources are terminated by the user on the self-service basis.

3.3.10. The user can request assistance from Cloud Support team in case they encounter any issues with VMs termination.

3.3.11. In exceptional/emergency cases, Cloud Support team can restore a terminated VM from the recycle bin within 7 days after the VM termination.

3.3.12. In case a user leaves a project or is dismissed, SSH keys belonging to them should be removed or passed to other active users within 7 days. Project Manager is responsible to verify that all keys were properly removed or passed.

3.4 NETWORK SECURITY

3.4.1. By default, all the VMs run in EPAM regions, are created in a default VLAN (Virtual Local Area Network).

3.4.2. EPAM Cloud Support team can move a VM to a custom VLAN by request. After a VM is moved to a custom VLAN, it cannot be returned to the default one.

3.4.3. By default, Cloud VMs in EPAM regions are available only from EPAM network.

3.4.4. VMs can be exposed to Internet by request to EPAM Service Desk, according to one of the scenarios, described by the Security Department, and available in EPAM knowledge base by this link.

3.4.5. The user should review the exposure scenarios and perform all the necessary preparations before submitting the exposure request.

3.4.6. The exposure of a VM to Internet is performed according to the following procedure:

a. The Security Department verifies that the VM meets all the Cloud and Corporate security requirements.

b. In special cases, Security Department verifies additional security-related solutions and approaches.

c. Cloud Support team places the VM to the DMZ.

d. Cloud Support team assigns an external IP, provided by EPAM Network team, to the VM. The connection details are sent to the VM Owner via email.

3.4.7. Once a VM is exposed to Internet, any new application on this VM must pass a security check.

3.4.8. Each service, port, or application, which is assumed to be exposed through a cluster/load balancer/proxy service, must pass a security check before the exposure.

3.4.9. It is strictly forbidden to expose non-controlled proxy servers.

3.5 EVENTS AUDIT

3.5.1. EPAM Orchestrator logs all the events related to users' actions in EPAM Cloud, performed via CLI, API, or Cloud UI.

3.5.2. The information about the events is stored during 100 days.

3.5.3. The user can access the information on the events in their projects with both Maestro CLI and Cloud UI.

3.5.4. EPAM Orchestrator does not store logs on events that were performed bypassing Orchestrator.

3.5.5. Cloud Support team can address AWS, Azure, or GCP Support to request help in investigating events that were performed bypassing Orchestrator.

3.6 USING EXTERNAL CLOUD PROVIDERS

3.6.1. User's access to an external platform's facilities is possible only after the activation of the respective project on this platform. The activation is performed by request and after the approval of the project's manager or coordinator.

3.6.2. The access to external Cloud providers' facilities via EPAM Orchestrator is enabled with Cloud UI and Maestro CLI by the same credentials as those used for private EPAM regions.

3.6.3. The access to native tools of external Cloud providers is provided by request to the users who have respective permissions, and if it is justified by project needs.

3.6.4. People who got access to native tools of external Cloud providers are personally responsible for the access credentials (login/password) to these tools.

3.6.1 Security in AWS

3.6.1.1. All VMs created in AWS are not available from outside EPAM network by default.

3.6.1.2. All VMs created in AWS, by default, have a set of security groups which allow to access these VMs from EPAM Offices. One security group is dedicated to custom rules, set up according to project needs.

3.6.1.3. In emergency cases, the Cloud Support team can edit or remove a custom security group without preliminary notice, if this group carries a security threat to the Cloud-based infrastructure.

3.6.1.4. VMs can be exposed to Internet by request to EPAM Service Desk. The exposure is performed in following steps:

a. The Security Department verifies that the VM meets all the Cloud and Corporate security requirements.

b. In special cases, Security Department verifies additional security-related solutions and approaches.

c. To establish access from Internet, Cloud Support team sets up the VM's security groups.

3.6.1.5. Security group changes can be performed either by request to Cloud Support team or by users who have an IAM user with the respective permissions.

3.6.1.6. By default, each account in AWS has a set of pre-defined IAM permission settings.

3.6.1.7. Custom IAM permission settings can be applied by request to the Cloud Support team. Security Department approval is needed for this operation.

3.6.1.8. In emergency cases, the Cloud Support team can edit IAM permission settings without preliminary notice, if these settings carry a security threat to the Cloud-based infrastructure.

3.6.1.9. A user can get access to AWS management console via AWS STS service, or by requesting an IAM user access.

3.6.1.10. The AWS access via AWS STS service provides the user with the permissions, determined by their project roles.

3.6.1.11. IAM user access to AWS can be granted temporarily (automatically by a respective call to Orchestrator, if the user has the respective permission) or permanently (by request to Cloud Support team, after approval from the respective Project Manager).

3.6.1.12. Temporary IAM access to AWS is cancelled after 60 minutes idle.

3.6.1.13. IAM User credentials should be rotated each 90 days. The password should not be repeated within latest 3 iterations.

3.6.1.14. The password should be generated randomly and meet the following requirements:

a. Include at least 14 characters

b. Include at least one upper case

c. Include at least one lower case

d. Include at least one number

e. Include at least one non-alphanumeric character

3.6.1.15. Permanent IAM User accounts must have multi-factor authentication mechanism activated. Virtual MFA device and standard DUO Mobile application are recommended for this purpose.

3.6.1.16. In case a permanent IAM User account does not have multi-factor authentication activated, EPAM Cloud Support teams can block (delete) it without preliminary notice.

3.6.1.17. By default, IAM users have no permissions to create IAM users and manage security groups. The creation of new IAM users (including IAM roles creation) and security groups management are under the responsibility of the Cloud Support groups with close cooperation with the Security Department.

3.6.1.18. Additional permissions can be granted to IAM users only by grounded request.

3.6.1.19. All IAM User names should comply with the syntax: <domain_name>@epam.com.

3.6.1.20. Any IAM User should be assigned to a unit (project member or auto user) belonging to a specific project, which is marked in UPSA as active.

3.6.1.21. An IAM user access owner is responsible for all actions performed under their IAM user account, and their consequences.

3.6.1.22. In case a permanent IAM user account is inactive for over 30 days, it can be removed, with prior notification to the IAM account owner.

3.6.1.23. Authorization to Linux instances can be performed only via SSH keys.

3.6.1.24. EPAM Cloud Team and Security Department can establish additional monitoring over events in AWS in order to detect threatening activities.

3.6.1.25. If Orchestrator detects unexpected or unusual events in AWS, a respective warning is sent to the project teams and Security Department and/or respective Cloud Support groups.

3.6.1.26. All abuse notifications from AWS should be answered immediately and resolved within one day. VM Owners, projects primary and secondary contacts are responsible for this.

3.6.1.27. Cloud Support team can block the project AWS account in case if an AWS abuse issue is not resolved within one day.

3.6.2 Security in Azure

3.6.2.1. A user can access virtual infrastructures in Azure via EPAM Orchestrator, if their project is activated in Azure via EPAM Cloud.

3.6.2.2. When a project is activated in Azure, a network security group is created for the new Azure subscription in order to allow access only for specified EPAM IP-addresses.

3.6.2.3. In emergency cases, the Cloud Support team can edit or remove a custom security group without preliminary notice, if this group carries a security threat to the Cloud-based infrastructure.

3.6.2.4. By default, each account in Azure has a set of pre-defined user permission settings.

3.6.2.5. Custom user permission settings can be applied by request to the Cloud Support team. Security Department approval is needed for this operation.

3.6.2.6. In emergency cases, the Cloud Support team can edit user permission settings without preliminary notice, if these settings carry a security threat to the Cloud-based infrastructure.

3.6.2.7. The user can get Azure AD-based access to the Azure portal, in terms of self-service, in case they have the respective permissions level.

3.6.2.8. The user's access to the project subscription in Azure is revoked within 24 hours after the user's project membership is cancelled.

3.6.2.9. Project VMs in one region are connected into one network so that they can reach each other by internal IPs.

3.6.2.10. EPAM Cloud Team and Security Department can establish additional monitoring over events in Azure in order to detect threatening activities.

3.6.2.11. All abuse notifications from Azure should be answered immediately and resolved within one day. VM Owners, projects primary and secondary contacts are responsible for this.

3.6.2.12. Cloud Support team can block the project Azure subscription in case if an Azure abuse issue is not resolved within one day.

3.6.2.13. Project VMs can be exposed to Internet by request to EPAM Service Desk. The exposure is performed in following steps:

a. The Security Department verifies that the VM meets all the Cloud and Corporate security requirements.

b. In special cases, Security Department verifies additional security-related solutions and approaches.

c. To establish access from Internet, Cloud Support team sets up the VM's security groups.

d. The access to Azure Portal is provided automatically for users by a respective call to Orchestrator, in case the user has the permissions to perform such call.

3.6.2.14. By default, users in Azure have no permissions to create other users and manage security groups. The creation of new users, roles, and security groups management are under the responsibility of the Cloud Support groups with close cooperation with the Security Department.

3.6.2.15. Additional permissions can be granted to Azure users only by grounded request.

3.6.2.16. All Azure user names should comply with the syntax: <domain_name>@epam.com.

3.6.2.17. Each Azure user should be assigned to a unit (project member or auto user) belonging to a specific project, which is marked in UPSA as active.

3.6.2.18. An Azure user access owner is responsible for all actions performed under their user account, and their consequences.

3.6.2.19. In case a permanent Azure user account is inactive for over 30 days, it can be removed, with prior notification to the IAM account owner.

3.6.2.20. Authorization to Linux instances can be performed only via SSH keys.

3.6.2.21. EPAM Cloud Team and Security Department can establish additional monitoring over events in Azure in order to detect threatening activities.

3.6.2.22. If Orchestrator detects unexpected or unusual events in Azure, a respective warning is sent to the project teams and Security Department and/or respective Cloud Support groups.

3.6.2.23. All abuse notifications from Azure should be answered immediately and resolved within one day. VM Owners, projects primary and secondary contacts are responsible for this.

3.6.2.24. All abuse notifications from Azure should be answered immediately and resolved within one day. VM Owners, projects primary and secondary contacts are responsible for this.

3.6.2.25. Cloud Support team can block the project Azure account in case if an Azure abuse issue is not resolved within one day.

3.6.3 Security in GCP

3.6.3.1. All VMs created in GCP are not available from outside EPAM network by default.

3.6.3.2. All VMs created in GCP are affected by the project firewall that allows accessing the VMs only from EPAM Offices (check by IP addresses).

3.6.3.3. In emergency cases, the Cloud Support team can edit or remove custom firewall rules without preliminary notice, if these rules carry a security threat to the Cloud-based infrastructure.

3.6.3.4. By default, each account in GCP has a set of pre-defined user permission settings.

3.6.3.5. Custom user permission settings can be applied by request to the Cloud Support team. Security Department approval is needed for this operation.

3.6.3.6. In emergency cases, the Cloud Support team can edit user permission settings without preliminary notice, if these settings carry a security threat to the Cloud-based infrastructure.

3.6.3.7. VMs hosted in GCP can connect to each other only by internal IP address or host name by default.

3.6.3.8. VMs can be exposed to Internet by request to EPAM Service Desk. The exposure is performed in following steps:

a. The Security Department verifies that the VM meets all the Cloud and Corporate security requirements.

b. In special cases, Security Department verifies additional security-related solutions and approaches.

c. The Cloud Support team sets up the firewall rules to establish access from Internet to the VM.

d. The access to GCP is provided automatically for users by a respective call to Orchestrator, in case the user has the permissions to perform such call.

3.6.3.9. By default, GCP users have no permissions to create other users and manage security groups. The creation of new users, roles, and firewall rules management are under the responsibility of the Cloud Support groups with close cooperation with the Security Department.

3.6.3.10. Additional permissions can be granted to IAM users only by grounded request.

3.6.3.11. All GCP user names should comply with the syntax: <domain_name>@epam.com.

3.6.3.12. Each GCP user should be assigned to a unit (project member or auto user) belonging to a specific project, which is marked in UPSA as active.

3.6.3.13. Firewall changes can be performed either by request to Cloud Support team or by users who have access to the GCP console.

3.6.3.14. The temporary access to the GCP can be retrieved by a user who has proper permissions, by a respective call to Orchestrator.

3.6.3.15. The user can get G-Suite-based access to Google Cloud Platform console, in terms of self-service, in case they have the respective permissions level.

3.6.3.16. The user access to a project is cancelled automatically within 24 hours after the account owner leaves this project, or by the Project Manager's request to the Cloud Support team.

3.6.3.17. A G-Suite account cannot be removed or suspended, unless the employee is dismissed.

3.6.3.18. EPAM Cloud Team and Security Department can establish additional monitoring over events in GCP in order to detect threatening activities.

3.6.3.19. If Orchestrator detects unexpected or unusual events in GCP, a respective warning is sent to the project teams and Security Department and/or respective Cloud Support groups.

3.6.3.20. All abuse notifications from GCP should be answered immediately and resolved within one day. VM Owners, projects primary and secondary contacts are responsible for this.

3.6.3.21. Cloud Support team can block the GCP project in case if an GCP abuse issue is not resolved within one day.

3.7 VULNERABILITIES DETECTION AND MANAGEMENT

3.7.1 Security checks

3.7.1.1. EPAM Cloud Support and Security Department can perform security check operations on users' assets in Cloud without advance notice.

3.7.1.2. Security checks of Cloud VMs and assets can be performed both manually (by Cloud Support teams and/or Security Department) or automatically (by tools and applications properly configured for this purpose).

3.7.1.3. All VMs in Cloud are subject to vulnerability assessment and penetration testing procedures, according to standard EPAM policies, defined in https://pal.epam.com/pal_method_plugin/guidances/whitepapers/resources/EPM-SPI_VulnerabilityAssessmentAndPenetrationTestingWIGLO.docx

3.7.1.4. Security checks can be performed according to the pre-defined set of rules, described in Annex A.

3.7.1.5. Security checks performed within VM exposure procedures are performed by the Continuous Vulnerability Management (CVM) team only.

3.7.1.6. Security check tools are approved by EPAM Global Information Security Head and Global IT Security Manager, and set up by Cloud Support L3 team and Security Department.

3.7.1.7. Security check procedures are defined and approved by EPAM Global Information Security Head.

3.7.1.8. Security check results are delivered to Cloud Support teams, the Continuous Vulnerability Management (CVM), and the responsible project persons (VM owners, primary and secondary contacts).

3.7.1.9. The security checks include checking the security groups and detecting those that can lead to security vulnerabilities (the rules are described in Appendix B).

3.7.2 Vulnerabilities management

3.7.2.1. VM owners, Project Managers, Delivery Managers, Project Coordinators are responsible for resolving issues and vulnerabilities detected on the VMs assigned to their projects.

3.7.2.2. If security scanning detects vulnerabilities or issues on Cloud VMs, the users related to problem resources get notified on this automatically, or manually.

3.7.2.3. Each user is responsible for fixing vulnerabilities and issues on their related resources in terms of self-service.

3.7.2.4. The urgency of issues and vulnerabilities resolving depends on the vulnerability/issue type:

a. Vulnerabilities:

- Critical: 3 days
- High: 7 days
- Medium: 30 days

b. Issues:

- Critical: 7 days
- High: 10 days
- Medium: 10 days

3.7.2.5. In case a user does not resolve the issue or vulnerability they are responsible for, the Continuous Vulnerability Management (CVM) team informs user's manager on the issue.

3.7.2.6. If necessary, the Continuous Vulnerability Management (CVM) provides consulting related to vulnerabilities and issues resolving, by appropriate request to EPAM Support Portal and within the scope of their responsibilities.

3.7.2.7. In case the reported issues or vulnerabilities are not fixed within the specified time, Cloud Support team and the Security Department can take security measures on the threat isolation. These measures can vary from instance isolation or suspension to full blocking, depending on the results of evaluation of the potential threat and the business needs.

3.8 CLOUD E-MAILS AND NOTIFICATIONS

3.8.1. EPAM Orchestration and Cloud support teams deliver Cloud-related notifications to the members of the projects, activated in Cloud, in order to assure sufficient informational support on the events, changes and issues (including security) related to EPAM Cloud in general, and project VMs, particularly.

3.8.2. Each notification is addressed to the users who can be influenced by the action, event, or issue described in the message, or to whom the provided information is considered to be important.

3.8.3. The members of the Advanced Management Group can delegate emails, sent to them as to the members of this group, to trusted users, in terms of self-service. When emails are delegated, the initial recipient stops receiving them.

3.8.4. The user can unsubscribe from notifications or set up filtering rules in their email client. In this case, the user is responsible for any consequences that result from the delivered information loss.

3.8.5. The user should keep to corporate information security rules, when they share the information and the materials delivered in Cloud-related emails.

ANNEX A – SECURITY SCANNING POLICIES

Policy Name	Policy Description	Scan Type
EPM-Srv-noWebApp-noCreds **(Default)**	The policy is configured for servers that do not host web applications. Operating system and Databases are checked. Web applications and networking equipment scanning is not included. No authorization is needed.	Black Box
Wrk-noCreds	The policy is configured for workstations scanning. Databases, networking equipment, web applications scanning is not included. Accounts are not used for scanning.	Black Box
Wrk-Creds	The policy is configured for workstations scanning. Databases, networking equipment, web applications scanning is not included. Local administrator account is used for scanning. Authorization allows to detect more issues on the target VM.	White Box
EPM-Srv-WebApp-noCreds	The policy is configured for web application servers check. Operating system, database, and web applications check is included. Networking equipment is not scanned. The procedure takes more time than the one where web applications are not scanned. No accounts are used for scanning.	Black Box
EPM-Srv-WebApp-Clickjacking	The policy is configured for web application servers check and provides quick urgent scanning of web applications for Clickjacking vulnerability only, with maximum page number and depths crawl. No authorization is needed for this type of scan. The policy is configured for web application servers check and provides quick urgent scanning of web applications for Clickjacking vulnerability only, with maximum page number and depths crawl. No authorization is needed for this type of scan.	Black Box
EPM-FULL-Creds_ANY_	The scanning is performed without any limitations and optimization measures. All elements are scanned. All accounts that have ever been created since the VM run, are used during the procedure. The whole procedure can take significant time.	White Box
EPM-Discovery	The policy is configured to perform quick scanning of any network range, in order to detect new assets and unauthorized devices. The scanning allows to create the network map. Vulnerabilities check is not performed.	Black Box
EPM-Srv-noWebApp-Creds*	The policy is configured for servers that do not host web applications. Operating system and Databases are checked. Web applications and networking equipment scanning is not included. Different accounts are used for scanning.	White Box
EPM-Windows-Torrents*	The policy is configured for quick scanning Windows workstations and servers for torrents and P2P applications. No other vulnerabilities will be detected. Authorization is needed.	White Box

Policy Name	Policy Description	Scan Type
EPM-Srv-WebApp-Creds*	The policy is configured for web application servers check. Operating system, database, and web applications check is included. Networking equipment is not scanned. The procedure takes more time than the one where web applications are not scanned. Different accounts can be used for scanning.	White Box
EPM-Lan-Creds*	The policy is configured for networking equipment check. Operating system, databases, web applications are not scanned. Different accounts are used for scanning.	White Box
EPM_bitlocker*	The policy is configured to check whether Windows servers and workstations have encrypting enabled. Scanning can detect the encrypted disks and the TPM module. No other vulnerabilities checks are included. Scanning needs authorization.	White box
* These policies need authentication for scanning. If you want your VM be scanned with these policies, please submit a respective request to the Continuous Vulnerability Management (CVM) team.		

APPENDIX A. SECURITY GROUP CHECK RULES

During the security groups check, the following ports are reviewed:

Protocol	Port	Source	Recommendation	Checked source	Vulnerable
Inbound					
TCP/UDP	21	ANY (even if it will be exposed for particular IPs)	Don't use 21 port. EPAM has FTP servers that can be used for information exchange.	0.0.0.0/0	TRUE
				10.23.14.145/32	TRUE
				46.133.203.215/32	TRUE
	22	0.0.0.0/0	Expose to EPAM IPs only.	0.0.0.0/0	TRUE
				10.23.14.145/32	FALSE
				46.133.203.215/32	TRUE
	80	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	137	0.0.0.0/0	Expose to EPAM IPs only.	0.0.0.0/0	TRUE
				10.23.14.145/32	FALSE
				46.133.203.215/32	TRUE
	443	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	445	0.0.0.0/0	Expose to EPAM IPs only.	0.0.0.0/0	TRUE
				10.23.14.145/32	FALSE
				46.133.203.215/32	TRUE
	3389	0.0.0.0/0	Expose to EPAM IPs only.	0.0.0.0/0	TRUE
				10.23.14.145/32	FALSE
				46.133.203.215/32	TRUE
	6881	ANY (even if it will be exposed for particular IPs)	Don't use port 6881. EPAM prohibits exposing this port without exceptions	0.0.0.0/0	TRUE
				10.23.14.145/32	TRUE
				46.133.203.215/32	TRUE
	8000	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	8001	0.0.0.0/0	Expose to particular external IPs	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	8080	0.0.0.0/0		0.0.0.0/0	TRUE

Protocol	Port	Source	Recommendation	Checked source	Vulnerable
			Expose to particular external IPs.	46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	8081	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	9000	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	9443	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
ANY	rest of 0-65535	0.0.0.0/0	Define particular ports for exposing and external range of IPs.	0.0.0.0/0	TRUE
Outbound					
TCP/UDP	25	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	465	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	587	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	993	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	995	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	2525	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE
	2526	0.0.0.0/0	Expose to particular external IPs.	0.0.0.0/0	TRUE
				46.133.203.215/32	FALSE
				10.23.14.145/32	FALSE

REVISION HISTORY		
Ver.	**Description of Change**	**Date**
1.9	Split Security Team responsibilities into responsibilities by respective sub-teams. Added info about technical account on Linux. Clarified IAM users details	13-Jul-2020
1.8	Updated vulnerabilities fixes terms	31-Oct-2019
1.7	Updated IAM policies management, security scans info, shared responsibility model	10-Aug-2019
1.6	Specified EPAM Cloud consulting as a team, responsible for the policy review and update.	06-Mar-2018
1.5	QA review	05-Mar-2018
1.4	Reviewed access regulations. Updated permissions info. Added Simple User Account section. Updated Network Security section with exposure recommendations. AWS IAM users provisioning and management updated. Azure portal access details added. Security Groups	February, 2018
1.3	Added information on Service Accounts, providing access to external users, and updated details on credentials updates Updated information on Security Checks, added Appendix A and B	August, 2017
1.2	Updated with the GCP info	July, 2017
1.1	Updated with IAM users management details. Updated project contacts.	October, 2016
0.9	Updated with AWS-related changes	April, 2016
0.5	Prepared for publishing	April, 2016
0.1	Initial draft	March, 2016