Policy - Cloud Security

Introduction

This Policy aims to regulate secure usage of the cloud resources as a service within GlobalLogic aimed to support internal systems, services and applications to protect the integrity and confidentiality of the GlobalLogic information and the security of the corporate network.

1. Scope

This document is applicable to the cloud resources aimed to support GlobalLogic internal systems, services and applications. Policy pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), cloud Compute.

2. Responsibilities

Role	Responsibility
CISO	Responsible for authorizing the usage of the cloud services within GlobalLogic.
SOC	Responsible for- ● Cloud vendor security assessment ● Vulnerability assessment of cloud infrastructure ● Penetrating testing of cloud infrastructure ● Security/Gap assessment for cloud infrastructure ● Logs monitoring
IT Infrastructure Team	Responsible for- ● Cloud resource management ● Access management ● System/ network health management
Information Security Team	Responsible for auditing security controls are adequately implemented

Abbreviations and Definitions

Abbreviation/Definition	Description
Software-as-a-Service (SaaS)	A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. The infrastructure, software, and data are primarily the responsibility of the provider, since the customer has little control over any of these features.
Infrastructure-as-a-Service (IaaS)	A form of cloud computing that provides virtualized computing resources over the Internet. The provider is supplying and responsible for securing basic IT resources such as machines, disks, and networks. The customer is responsible for the operating system and the entire software stack necessary to run applications and is responsible for the customer data placed into the cloud computing environment. This means most of the responsibility for securing the applications and the data falls onto the customer.
Platform-as-a-Service (PaaS)	A cloud computing service that provides a platform allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application. Responsibility is likely shared between the customer and provider.
CISO	Chief information Security Officer
ISO	Information Security Officer
SOC	Security Operation Center
SSO	Single Sign On
CSP	Cloud Service Provider

3. Description

1. Only authorized cloud services shall be used for work purposes - GL or client provided. Personal cloud services accounts must not be used for the storage, manipulation or exchange of company-related communications or company and client(s)-owned information.
2. Cloud vendors shall meet basic Information Security requirements, stated in the Policy - Information Security Requirements to Third Party Vendors.
3. ISO shall undertake relevant risk assessments to identify the risks associated with using the cloud service. Any residual risks connected to the use of the cloud service should be clearly identified and accepted by the appropriate management of the GlobalLogic.

4. GlobalLogic will specify the Geo locations for data storage and should be approved by the compliance and privacy team accordingly.
5. The use of cloud services must comply with the Policy - Acceptable Use.
6. Employees/consultants must not share log-in credentials with anyone as stated in the Policy - Password Management.
7. Access management to the cloud resources shall be regulated by the Policy - Access Control.
8. GlobalLogic will formulate the “Naming convention” for cloud assets management.
9. The use of cloud services must comply with all laws and regulations governing the handling of personal data as set in the Policy – Privacy and Personal Data Protection Policy.
10. Data stored in the cloud shall be classified and labeled in accordance with the Policy - Information Classification, Labeling and Handling.
11. SSO and multi-factor authentication shall be implemented for accessing the cloud infrastructure.
12. Encryption on data at rest and in transit shall be implemented in accordance with the Policy - Cryptography.
13. GlobalLogic shall inventoried all cloud assets as per the Policy - Hardware Asset Management.
14. Cloud resources shall be hardened in line with industry best practices and vendor(s)’ recommendations.
15. GlobalLogic shall ensure logging is enabled in accordance with the Procedure - IT Monitoring.
16. Periodic Vulnerability assessment shall be conducted and patch management shall be done accordingly by respective teams.
17. Yearly Penetration testing shall be conducted to ensure that application and infrastructure is secure from any potential cyber attack.
18. GlobalLogic shall train its responsible staff on cloud technologies in use.
19. GlobalLogic shall maintain close contact with its cloud service provider(s). These contacts enable mutual exchange of information about information security for the use of the cloud services including a mechanism for both cloud service provider and the GlobalLogic to monitor each service characteristic and report failures to the commitments contained in the agreements.

Change History

Revision	Change Description	Review Date	Approver
1.0	Initial version of the document	06/18/2022	Alok Malik (CISO)
1.1	Point 12 was removed from section 3. Description	07/07/2023	Denys Kudriavchenko, Head of Security Risk & Compliance
1.2	Updated name and link for Policy - Asset Management	09/19/2023	Denys Kudriavchenko, Head of Security Risk & Compliance