This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Cloud Computing and Hosting Cybersecurity Policy Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously.
- Enter “<organization name>” in the Find text box.
- Enter your organization’s full name in the “Replace” text box.
- Click “More”, and make sure “Match case” is ticked.
- Click “Replace All”.
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This policy aims to define the cybersecurity requirements related to the protection of <organization name>'s information and technology assets on cloud computing services and hosting to achieve the main objective of this policy which is minimizing the cybersecurity risks resulting from internal and external threats at <organization name> in order to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all <organization name>'s information and technology assets on cloud computing services, which are hosted, processed, or/and managed by third parties, and applies to all personnel (employees and contractors) in the <organization name>. The implementation of requirements in this policy is dependent on the type of cloud computing services provided to <organization name>.

Policy Statements

1 General Requirements

1-1 Cybersecurity roles, including Responsible, Accountable, Consulted, and Informed (RACI), must be defined for all stakeholders in cloud computing services.

1-2 Cybersecurity risks must be managed following a methodological approach to protect the date and information and technology assets hosted on cloud computing services, as per the relevant legal and regulatory requirements.

1-3 Cybersecurity risks of hosting applications and services on cloud computing must be assessed before selecting cloud computing and hosting service providers.

1-4 The efficiency and reliability of cloud computing service providers must be verified, in addition to guaranteeing compliance with the cybersecurity requirements for cloud computing issued by the NCA, as per the relevant legal and regulatory requirements.

1-5 The cloud computing service provider's license and official register in the Kingdom of Saudi Arabia must be verified as per the classification and register of the cloud computing authorities in the KSA.

1-6 The implementation of all third-party cybersecurity requirements in the Third-party Cybersecurity Policy for all cloud computing and hosting service providers must be monitored and ensured, as per <organization name>'s regulatory policies and procedures and the relevant legal and regulatory requirements.

1-7 Cybersecurity risks related to the cloud computing service provider personnel must be effectively addressed before, during, and upon the termination of their employment, as per the relevant legal and regulatory requirements.

1-8 An accurate inventory of information and technology assets hosted on cloud computing services must be developed to ensure their confidentiality, integrity, accuracy, and availability as per the relevant legal and regulatory requirements.

1-9 Access to cloud services must be restricted to authorized users only and reviewed periodically as per <organization name>'s approved identity and access management policy.

1-10 It must be ensured that the cloud computing service provider separated <organization name>'s environment (including virtual servers, networks, and databases) from the environments of other organizations.

1-11 It must be ensured that networks are protected against cybersecurity risks by, for example, isolating the cloud technology systems' network from other networks, as per the relevant legal and regulatory requirements.

1-12 Mobile devices used to access cloud services must be protected against cybersecurity risks. Critical information and data on these

mobile devices must be handled safely, and they must be deleted before disposing of the mobile devices containing them, as per the relevant legal and regulatory requirements.

1-13 Data protection, confidentiality, integrity, accuracy, and availability must be ensured as per the relevant legal and regulatory requirements.

1-14 Data and information in transit to, stored in, or in transit from cloud services must be encrypted using up-to-date encryption methods as per the national encryption standards and as per <organization name>'s approved data classification policy.

1-15 The effectiveness of the cloud computing service provider's vulnerability management must be assessed according to the type of the provided service as per the relevant legal and regulatory requirements.

1-16 Event logs must be enabled on <organization name>'s information and technology assets hosted on cloud computing services, as per the relevant legal and regulatory requirements.

1-17 The cloud computing and hosting service provider must provide <organization name> with the required tools and technologies to manage and monitor its cloud services.

1-18 The cloud computing service provider must manage keys in accordance with <organization name>’s key management cybersecurity requirements, as per its key management standard/policy and the relevant legal and regulatory requirements.

1-19 The availability of cybersecurity resilience requirements in business continuity management must be guaranteed as per the relevant legal and regulatory requirements.

1-20 <organization name> must have the right to conduct cybersecurity tests and assessments on the cloud computing and hosting service provider or request the reports and results of cybersecurity assessments carried out by independent and trusted entities, and it must be guaranteed that this clause is included in the contracts signed with the cloud computing and hosting service provider.

1-21 <cybersecurity function> and <legal organization> must include <organization name>'s approved data hosting cybersecurity requirements in the contracts of cloud computing and hosting service providers as per the relevant legal and regulatory policies and requirements.

1-22 Procedures to use cloud computing services must be developed, documented, and approved.

1-23 Key performance indicators (KPIs) must be used to ensure the continuous improvement and effective and efficient use of the protection requirements of information and technology assets hosted on cloud computing services.

2 Data Hosting/Storage Cybersecurity Requirements

2-1 Data must be classified as per the relevant legislation and regulations before being hosted/stored by cloud computing and hosting service providers.

2-2 A formal and documented statement must be obtained from the cloud computing and hosting service provider regarding the level of license granted to it by the competent entities to host data based on the data classification. The cloud computing and hosting service provider must host and process <organization name>'s classified data only as per the granted license.

2-3 Cloud computing and hosting service providers must be required to return data (in a usable format) and delete them in an irreversible manner upon service termination/expiration, and it must be guaranteed that this clause is included in the contracts signed with the cloud computing and hosting service provider.

2-4 Cloud computing and hosting service providers must conduct periodic tests to verify backup's recovery effectiveness.

2-5 <organization name>'s information hosting and storage location must be inside the Kingdom of Saudi Arabia taking into consideration the legal and regulatory requirements stipulating that such data must not be subject to the laws of any other countries.

2-6 Critical systems or any of their technical components must be hosted inside <organization name>'s premises or on cloud computing service provided by a government entity or a national company that meets NCA's cloud computing and hosting service controls, while considering the classification of the hosted data.

Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>
2- **Policy Review and Update:** <cybersecurity function>
3- **Policy Implementation and Execution:** <information technology organization> and <cybersecurity function>
4- **Policy Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- <head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.
2- All personnel of <organization name> must comply with this policy.
3- Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.