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.

Third-Party 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 against cybersecurity risks related to third parties, including information technology outsourcing and managed services.

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 information and technology assets and all the services provided to <organization name> by third parties and their personnel, including information technology outsourcing and managed services, and it applies to all personnel (employees and contractors) in <organization name>.

Policy Statements

1 General Requirements

1-1 Procedures must be documented, approved, and applied to manage <organization name>’s relation with third parties before, during, and after the end of the contractual relationship.

1-2 A cybersecurity risk assessment on third parties and provided services must be conducted, including but not limited to, reviewing third-party projects in <organization name>, periodically reviewing the cybersecurity event logs of third-party services (if possible) before and during the relation as per <organization name>'s approved Cybersecurity Risk Management Policy, and identifying the required protection controls that should be applied for the effective management of the detected cybersecurity risks.

1-3 Outsourcing and managed service companies that provide services to support or operate critical systems must undergo a vetting or screening process.

1-4 Contracts and agreements with third parties must include <organization name>'s cybersecurity requirements, as well as clauses binding the third parties to comply with <organization name>'s cybersecurity policies and other relevant legal and regulatory requirements.

1-5 Third-party personnel' contracts must include cybersecurity responsibilities and clauses of Non-Disclosure and secure deletion of <organization name>'s data (during and after the end or termination of the employment relationship with <organization name>).

1-6 It must be ensured that third parties manage their cybersecurity risks.

1-7 Third parties must grant <organization name> the necessary permissions to conduct tests to verify the third parties' compliance with <organization name>'s cybersecurity requirements and provide the required reports when needed.

1-8 Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and efficient and efficient application of third-party cybersecurity requirements.

2 Cybersecurity Requirements for Information Technology Outsourcing and Managed Services Provided by Third Parties

2-1 Third parties must be carefully selected for information technology outsourcing and managed services, and the following, as a minimum, must be verified:

2-1-1 A cybersecurity risk assessment must be conducted, and effective controls on risks must be ensured before signing contracts and agreements with third parties or if changes occur in relevant legal and regulatory requirements.

2-1-2 Cybersecurity managed service centers for operation and monitoring that use remote access must be completely present inside the Kingdom of Saudi Arabia.

2-1-3 Outsourcing services for critical systems must be provided by national companies and entities as per the relevant legal and regulatory requirements.

2-1-4 Outsourcing and managed services that deal with classified data must be provided by national companies and entities as per the relevant legal and regulatory requirements.

3 Cybersecurity Requirements for Third Party Personnel

3-1 Outsourcing and managed service companies and their personnel working on critical systems and having classified data access must undergo screening or vetting.

3-2 Third-party personnel who are expected to have direct or indirect access to <organization name>'s assets must sign an undertaking to protect information confidentiality before starting the work relation, as per the format approved by <organization name>.

3-3 Third-party personnel must be educated about <organization name>'s cybersecurity requirements, and their compliance must be ensured.

4 Cybersecurity Requirements for Authentication and Access Controls

4-1 Third parties must develop approved procedures to grant and revoke access to all information and technology systems that process, transmit, or store <organization name>'s information, in line with <organization name>'s cybersecurity requirements and the objectives the cybersecurity controls.

4-2 Third-party personnel access to <organization name>'s information must be restricted, and information must be processed securely, while ensuring continuous monitoring of access processes.

4-3 Password controls must be implemented for all users with access to <organization name>'s information in line with <organization name>'s cybersecurity requirements and the objectives the cybersecurity controls.

4-4 Access rights must be revoked upon the end/termination of the service of any third-party employee with access to <organization name>'s information or information and technology assets or in the event of a change in their job role that eliminates the need for continued access.

4-5 Third parties must review access rights regularly as per <organization name>'s approved Identity and Access Management Policy.

4-6 Audit records must be securely stored, maintained, and made available at <organization name>'s request and as per the relevant legal and regulatory requirements.

5 Change Management Cybersecurity Requirements

5-1 Third parties must follow a formal and appropriate change management process as per <organization name>'s policies and procedures.

5-2 Changes to <organization name>'s information and technology assets must be reviewed and tested before their implementation in the production environment.

5-3 Major changes planned or introduced to <organization name>'s information and technology assets must be communicated to <organization name>'s relevant stakeholders.

6 Cybersecurity Incident Management and Business Continuity Requirements

6-1 Third-party contracts and agreements must include requirements related to cybersecurity incident reporting and informing <organization name> of any cybersecurity incident that the third-party faces.

6-2 Communication procedures between third parties and <organization name> must be defined and documented, to be used in case of any cybersecurity incident that the third-party faces or to report vulnerabilities. These procedures must be reviewed and updated periodically.

6-3 An appropriate business continuity plan must be developed to avoid the unavailability of the services provided to <organization name> in line with <organization name>'s business continuity and disaster recovery plan requirements.

7 Data and Information Protection Requirements

7-1 <Organization name>'s information and data residing on all systems, and processed or stored by third parties, must be

classified according to <organization name>'s approved Data Classification Policy.

7-2 Third parties must process, store, and destruct <organization name>'s information and data according to <organization name>'s approved Data and Information Protection Policy and Standard.

7-3 Third-party contracts and agreements must include the ability to securely delete the <organization name>'s data at the third party's side at the end or termination of the contractual relationship, with the provision of evidence of such deletion.

7-4 Third parties must apply appropriate encryption controls to protect information and data based on their classification at <organization name> and ensure their confidentiality, integrity, and availability in line with <organization name>'s approved Cryptography Standard.

7-5 Third parties must regularly back up <organization name>'s information and data as per <organization name>'s Backup and Recovery Management Policy.

7-6 <organization name>'s information and data residing in critical systems and personal data processed by third parties must not be processed, stored, or used in the testing environment unless restrict controls are applied to protect such data, such as data masking, data scrambling, or data anonymization, and after obtaining the necessary approvals from the concerned departments in <organization name> to ensure data protection and privacy as per the guidelines and requirements of the National Data Management Office (NDMO).

7-7 <organization name>'s information and data residing in critical systems and processed or stored by third parties must not be transmitted out of the production environment.

8 Audit

8-1 <organization name> must audit any related processes and systems whenever deemed necessary or appropriate.

8-2 Third-party personnel must be fully cooperative with <organization name>'s event log review and audit activities including implemented reviews.

Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <cybersecurity function>, <information technology function> <human resources function>, <legal affairs function>, and <procurement 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.