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.

Human Resources Cybersecurity Policy Template

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.

Choose Classification

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

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 legal 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 text

Table of Contents

Purpose

This policy aims to define the cybersecurity requirements related to personnel in <organization name> in order to minimize the cybersecurity risks resulting from internal and external threats 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 applies to all personnel (employees and contractors) in <organization name>.

Policy Statements

1- General Requirements

1-1 Limit and approve cybersecurity requirements related to personnel before, during and at the end/termination of employment at the organization.

1-2 The <organization name> must conduct cybersecurity awareness campaigns for all personnel.

1-3 Review cybersecurity requirements related to <human resources> at least once a year including the controls related to the organization personnel on a regular basis. Any changes must be documented and approved by the organization representative then update this policy accordingly.

1-4 Fill critical systems related functions in the <organization name> with highly qualified Saudi nationals.

1-5 Define knowledge, skills and capabilities required for different cybersecurity functions accurately.

1-6 Fill cybersecurity functions with qualified Saudi nationals in cloud computing service provider's data centres within the Kingdom of Saudi Arabia.

1-7 Implement human resources cybersecurity controls throughout the employee's lifecycle in <organization name>, which includes the following phases:

1-7-1 Pre-employment

1-7-2 During service period

1-7-3 At the end or termination of employment

1-8 Implement cybersecurity requirements related to the personnel responsible for managing and maintaining social media accounts as per cybersecurity policies, procedures and processes of social media accounts.

1-9 Personnel of <organization name> must understand and agree on their job roles, cybersecurity requirements and responsibilities.

1-10 Ensure that cybersecurity risks related to personnel (employees and contractors) of cloud computing service providers and cloud computing service subscribers are effectively addressed before, during, and at the end/termination of employment, in accordance with the policies and regulatory procedures, and relevant legal and regulatory requirements.

1-11 Include responsibilities of cybersecurity and Non-Disclosure Agreement clauses in the contracts of <organization name> personnel (to be included during and after the end/termination of employment with <organization name>).

1-12 Include cybersecurity violations in the Human Resources violations regulation in <organization name>.

1-13 Personnel information must not be accessed without prior authorization.

1-14 Use Key Performance Indicator (KPI) to ensure continuous improvement and proper and effective use of cybersecurity requirements related to human resources.

2- Pre-employment

2-1 Personnel must undertake to comply with cybersecurity policies before being granted access to <organization name> systems.

2-2 Employee roles and responsibilities related to cybersecurity must be defined in job description, taking into account the application of non-conflict of interest's principle.

2-3 Cybersecurity roles and responsibilities must include the following:

2-3-1 Protect all <organization name> assets from unauthorized access or vandalizing those assets.

2-3-2 Implement all required cybersecurity related activities.

2-3-3 Comply with <organization name> cybersecurity policies and standard.

2-3-4 Adhere to the cybersecurity risk awareness program.

2-4 Approve and sign all cybersecurity policies by personnel as a prerequisite for accessing cloud-based technology systems.

2-5 Conduct security screening to personnel in cybersecurity functions, privileged access technology functions, and critical systems functions.

2-6 Conduct security screening to personnel with access to cloud computing services critical tasks such as key management, service management and access control.

3- During Employment:

3-1 Offer an awareness program to all <organization name> personnel to increase the level of cybersecurity awareness periodically.

3-2 Provide cybersecurity awareness through all available channels used in the <organization name> including social media accounts of <organization name>.

3-3 The <human resources function> must inform the relevant functions of any change in roles or responsibilities of personnel to take the necessary actions related to access cancellation or modification.

3-4 Ensure that all human resources cybersecurity requirements are applied.

3-5 Include the extent of cybersecurity compliance in employee assessment aspects.

3-6 Apply need-to-know principle in task assignment.

4- End or Termination of Employment:

4-1 Define employment expiry or termination procedures in a manner covering cybersecurity requirements.

4-2 The <human resources function> must inform the relevant units in case employment expiry or termination to take the necessary actions.

4-3 Ensure that all <organization name> assets are returned and personnel access rights are cancelled on their last working day and prior to obtaining the necessary clearance.

4-4 Define responsibilities and duties that will remain in effect after personnel end of employment in <organization name>, including the information confidentiality agreement, provided that such responsibilities and duties are included in all personnel contracts.

Roles and Responsibilities

1. **Policy Owner:** <head of cybersecurity function>
2. **Policy Review and Update:** <cybersecurity function>
3. **Policy Implementation and Execution:** <human resources 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- The <head of the cybersecurity function> will ensure 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 as per <organization name>'s procedures.