

1.8.1 Cybersecurity in Human Resources

Contents

1. Definitions	2
2. Purpose	2
3. Scope	2
4. Policy	3
5. Non-compliance	4
6. References	4

Version	Adjustment Date	Approved By	Approval Date and signature
2.1	19-6-2025	Saud Alsulami	19-6-2025



1. Definitions

For purposes of this “Cybersecurity in Human Resources” the following definitions apply:

- **Cyber incident:** an actual or imminent event or action that threatens or compromises the confidentiality, integrity, or availability of information systems or data. It includes security breaches, unauthorized access, data loss, or system disruptions.
- **Personnel:** all individuals working for or associated with the organization, including employees, contractors, and temporary staff. They are responsible for adhering to the organization's cyber security policies and practices.
- **Security culture:** the shared values, beliefs, and behaviors within an organization that promote a strong security posture. It involves fostering a sense of ownership, accountability, and proactive cyber security practices among personnel.

2. Purpose

The objective of the Cybersecurity Policy for Human Resources is to establish a comprehensive framework for managing cybersecurity risks associated with personnel in Taqnyat. This policy aims to set forth requirements and guidelines to ensure the selection of trustworthy and competent employees, raise awareness about cybersecurity, and implement best practices throughout their employment lifecycle. The policy also aims to protect Taqnyat's information assets, maintain the confidentiality of sensitive data, and foster a culture of cybersecurity awareness among employees.

3. Scope

The Cybersecurity Policy for Human Resources applies to all personnel, including permanent, temporary, and contract employees, who are currently employed or may be employed in the future by Taqnyat.



4. Policy

4.1. Pre-Employment Cybersecurity Requirements:

- Defining Cybersecurity Requirements: Before employing individuals, including contractors, clearly define and document the cybersecurity requirements they must meet. This includes specifying the necessary security clearances, background checks, and technical competencies for their respective roles.
- Background Verification Checks: Conduct comprehensive background verification checks on all candidates for employment. This includes criminal records checks, employment history verification, and reference checks. Prioritize candidates who demonstrate a strong commitment to cybersecurity and ethical behavior.
- Critical Systems Personnel: For positions related to critical systems, hire highly professional and qualified personnel with specialized cybersecurity expertise and a proven track record of maintaining secure environments.

4.2. During Employment Cybersecurity Requirements:

- Employment Terms and Agreements: Ensure that employment contracts or agreements explicitly cover cybersecurity responsibilities and expectations. Include non-disclosure agreements (NDAs) to protect sensitive information, both during and after employment.
- Code of Conduct: Establish a comprehensive code of conduct that outlines cybersecurity practices, ethical standards, and acceptable use policies for information assets. Ensure that all personnel, including contractors, sign and adhere to this code of conduct throughout their employment.
- Acceptable Use of Information Assets: Enforce an "Acceptable Use of Information Assets" policy that defines appropriate usage guidelines for organizational information systems and data. This policy should cover topics such as password management, data handling, remote access, and incident reporting.
- When an employee transitions to a new job position, any necessary modifications related to their new role are made based on a request from the Human Resources Department. The NOC or technical support department executes these changes and informs both the branch manager and the cybersecurity officer.



4.3. Post-Employment Cybersecurity Requirements:

- Termination Procedures: Upon completion or termination of employment, ensure that all access to organizational systems and data is promptly revoked. Conduct exit interviews to remind departing personnel of their ongoing confidentiality obligations and the consequences of unauthorized disclosure or misuse of information.
- Ongoing Confidentiality: Reinforce the importance of maintaining confidentiality even after employment ends. Highlight the legal and ethical implications of breaching non-disclosure agreements and emphasize the potential consequences, including legal action and damage to professional reputation.

4.4. Continuous Measurement, Review, and Optimization:

- Regular Training and Awareness: Provide regular cybersecurity training and awareness programs to keep personnel informed about evolving threats, best practices, and their cybersecurity responsibilities. This helps ensure a strong security culture within the organization.
- Policy Review and Update: Periodically review and update this cybersecurity policy to reflect changes in technology, threats, and regulatory requirements. Stay informed about emerging cybersecurity trends and incorporate relevant industry best practices.
- Incident Response and Reporting: Establish clear procedures for reporting and responding to cybersecurity incidents involving personnel. Encourage a culture of open communication and prompt reporting to facilitate effective incident handling and mitigation.

5. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

6. References

- ISO 27002
- National Cybersecurity Authority's (NCA) ECC standards