

2.1.1 Asset Discovery

Contents

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

Version	Adjustment Date	Approved By	Approval Date
2.0	4/7/2024	Saud Alsulami	7/7/2024

1. Definitions

For purposes of this "Asset Discovery policy" the following definitions apply:

- **IT Asset:** is any valuable component within the information technology infrastructure of an organization. This can include hardware devices, software applications, data, networks, and other elements that contribute to the management, processing, and storage of information.
- **Asset Inventory:** a comprehensive and up-to-date listing of all organizational assets, including IT assets. It involves the systematic documentation of hardware, software, data, personnel, and other resources, along with relevant details such as ownership, classification, and location.
- **Asset Owner:** an individual or entity responsible for the overall management, protection, and decision-making regarding a specific asset within the organization.
- **Unauthorized asset:** any information technology asset, including hardware, software, or data, that is present within an organization's infrastructure without proper authorization, approval, or documentation.

2. Purpose

To establish a set of guidelines and procedures for the systematic identification, classification, and management of information assets within Taqnyat environment.

3. Scope

All information assets, within the organization. It applies to all hardware, software, and information used by Taqnyat.

4. Policy

- 4.1. The asset inventory must be established and updated by the NOC department.
- 4.2. The asset management application, Snipe-IT, is utilized by Taqnyat to manage its assets effectively.
- 4.3. When an asset is purchased or transferred, its information must be updated in the application within a maximum of three business days.
- 4.4. The NOC department must implement a comprehensive asset discovery process to identify all information assets.

- 4.5. Asset discovery shall be conducted regularly and be integrated into the overall risk management process.
- 4.6. The NOC team must maintain an up-to-date inventory of all identified assets, including relevant details such as ownership, classification, and criticality.
- 4.7. All assets must have an asset owner, and he will be responsible for protection and maintenance.
- 4.8. The asset inventory list encompasses all physical assets, including employee devices, printers, servers, network devices, and software licenses.
- 4.9. An asset discovery program must automatically search at least daily.
- 4.10. The asset list is updated based on the new assets discovered within 48 hours.
- 4.11. It is necessary to verify the ownership and information of the assets before entering them into the asset inventory list.
- 4.12. Asset inventory must include the following information: asset name and type, asset owner, serial number, and asset classification.
- 4.13. Assets under maintenance should be distinctly identified to ensure proper follow-up.
- 4.14. The cybersecurity department conducts yearly audits to ensure compliance with policies and procedures.
- 4.15. Upon discovering any unauthorized or unknown asset, appropriate action must be taken to mitigate security risks (like turn-off the asset — block network access — remove software).
- 4.16. In the event of discovery of any asset not listed in the asset management application, a non-compliance report is submitted to the CEO.

5. Non-compliance

Non-compliance with this policy could expose Taqnyat company to risks. Therefore, the discovery of any unauthorized equipment by the NOC team may subject the responsible party to graduated penalties based on the severity of the violation.



6. References

- ISO 27002
- National Cybersecurity Authority's (NCA) ECC standards
- SANS v7.0



Internal Use Only