

2.2.1 Asset Classification

Contents

1. Definitions	2
2. Purpose	2
3. Scope	2
4. Policy	2
5. Handling Asset Classification	3
6. Non-compliance	4
7. References	4

Version	Adjustment Date	Approved By	Approval Date and signature
2.1	18/12/2025	Saud Alsulami	2/1/2025



1. Definitions

For purposes of this “Asset Classification” the following definitions apply:

- **Confidentiality:** the protection of sensitive information from unauthorized access, disclosure, or use.
- **Integrity:** maintaining the accuracy, consistency, and reliability of data over its entire lifecycle. It ensures that data remains unchanged and unaltered by unauthorized or unintended means, such as errors or malicious activities.
- **Availability:** the accessibility and usability of systems, services, or data. It ensures that authorized users can access the information or resources they need when required, without experiencing undue delays or disruptions.
- **Asset Owner:** an individual or entity responsible for the overall management, protection, and decision-making regarding a specific asset within the organization.

2. Purpose

The objective of the Asset Classification Policy is to categorize and protect organizational assets according to their significance. This aims to ensure the implementation of specific security measures, compliance with regulations, and the efficient allocation of resources to minimize risks and safeguard sensitive information.

3. Scope

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

4. Policy

- 4.1. Assets must be classified based on their potential impact on the Taqnyat services, and the sensitivity of the information they handle.
- 4.2. The classification of assets shall be reviewed quarterly, and the classification shall be amended if it is not aligned with the established policies and procedures.
- 4.3. Asset classification must be based on three elements:
 - Confidentiality
 - Integrity
 - Availability
- 4.4. NOC department must identify and classify the assets.



- 4.5. Asset owners must be using the asset as the Acceptable Use of Information Assets policy.
- 4.6. The cyber security officer must provide guidance on the appropriate classification of assets.
- 4.7. Assets must be classified into three categories: low, medium, and high.
- 4.8. The low asset classification is typically handled routinely, like transfer of the asset by the operations department after ensuring the proper handling of information based on the asset disposal policy.
- 4.9. In case of any asset change (like transfer, return, disposal, delete) for the medium asset classification, approval from the asset owner must be obtained.
- 4.10. Any asset changes to high level assets must be carried out through the Change Management Policy, and no changes should be made without obtaining the necessary approvals.
- 4.11. This policy shall be reviewed annually

5. Handling Asset Classification

Assets have three classifications, low, medium, and high.

They are determined based on grades, and these grades are as follows:

- Confidentiality Impact:
 - “1” = Low impact (Public)
 - “2” = Medium impact (Internal Use Only)
 - “3” = High impact (Confidential)
- Integrity Impact:
 - “1” = Low impact (Limited damage)
 - “2” = Medium impact (Significant damage)
 - “3” = High impact (Severe damage)
- Availability Impact:
 - “1” = Low impact (Limited disruption)
 - “2” = Medium impact (Significant disruption)
 - “3” = High impact (Extended disruption)



When summing up the three numbers, the asset is classified as follows:

From	To	Classification
1	3	Low
4	7	Medium
8	9	High

Examples:

Service	Confidentiality Impact	Integrity Impact	Availability Impact	Total
Database server	3	3	3	9 (High)
The secretary's computer	1	1	0	2 (Low)

6. Non-compliance

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

7. References

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

