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 entity logo by clicking on the outlined image.



# Asset Classification Standard 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 standard aims to define the detailed cybersecurity requirements related to the asset classification of <organization name>'s systems, data and information to minimize cybersecurity risks resulting from internal and external threats at <organization's name> in order to preserve confidentiality, integrity and availability.

The requirements in this standard 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 standard covers all assets (e.g., physical, data, business application, software and technology assets) in the <organization name> and applies to all personnel (employees and contractors) in the <organization name>.

# Standards

| 1 | Asset classification |
|---|---|
| Objective | To classify all assets owned and managed by the <organization name>. |
| Risk Implication | The lack of development and implementation of asset classification in <organization name>, will fail to protect assets by using improper protective measures, controls or handling critical assets incorrectly which may lead to exposure or breach. |
| Requirements | |
| 1-1 | All assets owned and managed by <organization name> must be classified. |
| 1-2 | Physical assets (e.g., network connection devices, IDS/IPS, storage assets and critical systems' peripherals) must be classified by reference to the highest classification of the |

| | |
|---|---|
| | information input, processed, stored or transmitted on the physical asset. |
| 1-3 | Business application and software assets must be classified by reference to the highest classification of the information input, processed, stored, transmitted or deleted by users of the application or software. |
| 1-4 | Third party and suppliers must be classified by reference to the highest classification of the information input, processed, stored, transmitted or deleted by the third party or supplier. |
| 1-5 | Any asset (information, physical, business application, software and third party and supplier) that inputs, processes, stores, transmits or deletes personal and/or sensitive information must be classified as “Critical”, “High”, “Moderate”, “Low” in addition to any other classification required. |
| 2 | Physical asset labelling |
| Objective | To label all physical assets owned by the organization |
| Risk Implication | Unlabeled assets can be difficult to track, monitor or return to <organization name>. An unlabeled asset may not be included in an asset register, which can lead to the asset not being updated or maintained in the appropriate manner. Unlabeled physical assets may be handled incorrectly, which may result in damage, theft or loss. |
| Requirements | |
| 2-1 | All physical assets owned by the organization must have a tamper-proof label attached. |
| 2-2 | The tamper proof label must show the unique identifier assigned to the asset in the asset register as a number, bar code or QR code. |
| 2-3 | The tamper proof label must contain a contact number. |

| | |
|---|---|
| 2-4 | The tamper proof label must not contain <organization name>, <organization name> logo or other identifying marks or texts. |
| 3 | Physical asset handling |
| Objective | To protect assets by handling them in a secure manner. |
| Risk implication | Improper or careless handling of physical assets can lead to damage, loss or theft of the asset and any information stored or accessible on the device. Depending on the asset and information, <organization name> may be exposed to legal or regulatory investigations and penalties. |
| Requirements | |
| 3-1 | Physical assets (excluding assets recognized as mobile devices) must not be removed from their designated location. |
| 3-2 | Approval must be obtained from the asset owner if a physical asset is to be removed from its designated location. |
| 3-3 | Storage media, such as hard disk drives, that has been used to store classified information classified as “Top Secret”, “Secret”, “Confidential” must be securely erased using a published erasure method such that data cannot be retrieved (e.g., NIST SP800-88 Rev.1). |
| 3-4 | Storage, such as hard disk drives, that has been used to store classified information classified as classified information classified as “Top Secret”, “Secret”, “Confidential” must be physically destroyed (e.g. by shredding to Deutsches Institut für Normung (DIN) 66399 standard as O-5 and H-5 or incineration). |
| 4 | Mobile device physical asset handling |
| Objective | To protect mobile devices by handling them in a secure manner |

| | |
|---|---|
| Risk implication | Improper or careless handling of mobile assets can lead to damage, loss or theft of the asset and any information stored or accessible on the device. Depending on the asset and information, <organization name> may be exposed to legal or regulatory investigations and penalties. |
| Requirements | |
| 4-1 | Users of mobile devices (such as laptops, mobile phones and portable storage devices) that may input, process, store, transmit or delete classified data must be trained at least once a year in the secure handling of the devices and data. The users must acknowledge they have received and completed the training. |
| 4-2 | Mobile devices must be returned to a central location for disposal. |
| 4-3 | Storage, such as hard disk drives, in mobile devices that have been used to store classified information classified as “Top Secret”, “Secret”, “Confidential” must be securely erased using a published erasure method such that data cannot be retrieved following decommissioning (e.g. NIST SP800-88 Rev.1). |
| 4-4 | Storage, such as hard disk drives, in mobile devices that have been used to store classified information classified as “Top Secret”, “Secret”, “Confidential” must be physically destroyed following decommissioning (e.g., by shredding to DIN 66399 standard O-5 and H-5 or incineration). |
| 4-5 | Portable storage devices that have been used to store classified information must be physically destroyed following decommissioning (e.g., by shredding to DIN 66399 standard O-5 and H-5 or incineration). |
| 5 | Information asset labelling |
| Objective | To label information assets with their classification |

| | |
|---|---|
| Risk implication | Unlabeled information assets will not be handled correctly, raising the likelihood of exposure or breach. |
| Requirements | |
| 5-1 | Classified information assets in digital format (files, databases or emails) must be labelled electronically (e.g. by using headers and footers in documents, file naming conventions, or digital signatures). |
| 5-2 | Classified information assets in physical format (papers, hard copies, contracts, etc.) must be labelled using a tamper evident mechanism such as rubber ink stamps, adhesive labels and hologram lamination. |
| 5-3 | Classified information printed out in hard copy format from a business application or software must have the relevant classification applied before printing (according to the <organization name>'s Data Classification Policy). |
| 6 | Information asset handling |
| Objective | To handle information assets in a secure manner |
| Risk implication | Improper or careless handling of information assets may lead to exposure or a breach. Depending on the information exposed or breached, <organization name> may be exposed to legal or regulatory investigations and penalties. |
| Requirements | |
| 6-1 | Classified information assets in digital format must be encrypted during storage and transmission. |
| 6-2 | Electronic data or file transfers must be carried using an approved, secure, file transfer system (not email or other messaging application). |
| 6-3 | Data or files containing classified information must be transferred using a secure communication media, such as email over VPN or SFTP. |

| | |
|---|---|
| 6-4 | File transfer systems must require the use of a UserID. The file transfer system must log UserID, file transferred, date and time at a minimum. |
| 6-5 | File transfer system logs must be reviewed once a month by the Business Application Owner. |
| 6-6 | Classified information assets in physical format (papers, hard copies, contracts, etc.) must be protected by appropriate means at all times, such as being locked away when not in use and placed in envelopes when being transported. |
| 6-7 | Classified information assets in physical format must be locked away at the end of each working day, or if the desk is to be left unattended for longer than an hour. |
| 6-8 | Information assets classified as “Confidential” or below in physical format can be taken off <organization name> premises in a secure manner (e.g., placing the papers in a double envelope; ensuring no <organization name> identifiers can be seen; and placing the papers in a briefcase, laptop bag or hand luggage). |
| 6-9 | Information assets classified as “Confidential” or above in physical format cannot be taken off <organization name> premises. |
| 6-10 | Classified information assets in physical format sent to third parties or suppliers must be sent in a secure manner (e.g., placing the papers in a double envelope; ensuring no <organization name> identifiers can be seen; and placing the papers in a tamper-proof or tamper-evident package). |
| 6-11 | Classified information assets in physical format sent to third parties or suppliers must be sent using a courier or tracked mail method. The recipient must sign to acknowledge delivery. |

| | |
|---|---|
| 6-12 | Classified information assets in physical format must be securely destroyed by shredding —e.g., using a cross-cut shredder meeting DIN 66399 standard as P-4 or higher (such as P-5 or P-6). |
| 6-13 | Information assets in physical format classified as “Top Secret”, “Secret” must not be taken off <organization name> premises. |
| 6-14 | Information assets in physical format classified as “Top Secret”, “Secret”, “Confidential” must be securely destroyed by shredding (e.g., using a cross-cut shredder meeting DIN 66399 standard P-5 or P-6). |

# Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

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

3- **Standard Implementation and Execution:** <information technology function>

4- **Standard Compliance Measurement:** <cybersecurity function>

# Update and Review

<cybersecurity function> must review the standard 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 standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>’s procedures.

# Appendix

## A- Asset Classification Levels

| Classification Level | Description |
|---|---|
| Critical | <Asset is classified as “Critical”, if unauthorized access or misuse cause severe and exceptionally effects to the organization in a way that is difficult to resolve> |
| High | <Asset is classified as “High”, if unauthorized access or misuse causes significant effects to the organization> |
| Moderate | <Asset is classified as “Moderate”, if unauthorized access or misuse causes moderate effects to the organization> |
| Low | <Asset is classified as “Low”, if unauthorized access or misuse causes negligible or minor effects to the organization> |

## B- Data Classification Levels

| Classification Level | Description |
|---|---|
| Top Secret | <Data is classified as “Top Secret”, if unauthorized access or misuse cause severe and exceptionally effects to the organization in a way that is difficult to resolve> |
| Secret | <Data is classified as “Secret”, if unauthorized access or misuse causes significant or moderate effects to the organization> |
| Restricted | <Data is classified as “Restricted”, if unauthorized access or misuse causes minor or limited effects to the organization> |
| Public | <Data is classified as “Public”, if unauthorized access or misuse does not cause any effect to the organization> |