



AI (V1) Principle 13

1. ETSI

1.1. EN 304 223 - Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems

Link: https://www.etsi.org/deliver/etsi_en/304200_304299/304223/02.01.01_60/en_304223v020101p.pdf

Link: https://www.etsi.org/deliver/etsi_en/304200_304299/304223/02.01.01_60/en_304223v020101p.pdf

1.1.1. Provision 5.5.1-1

If a Developer or System Operator decides to transfer or share ownership of training data and/or a model to another entity they shall involve Data Custodians and securely dispose of these assets. This will protect AI against security issues that can transfer from one AI system instantiation to another.

1.1.2. Provision 5.5.1-2

If a Developer or System Operators decides to decommission a model and/or system, they shall involve Data Custodians and securely delete applicable data and configuration details.

1.2. TR 104 128 - Securing Artificial Intelligence (SAI); Guide to Cyber Security for AI Models and Systems

Link: https://www.etsi.org/deliver/etsi_tr/104100_104199/104128/01.01.01_60/tr_104128v010101p.pdf

Link: https://www.etsi.org/deliver/etsi_tr/104100_104199/104128/01.01.01_60/tr_104128v010101p.pdf

1.2.1. Provision 5.5.1-1

"If a Developer or System Operator decides to transfer or share ownership of training data and/or a model to another entity they shall involve Data Custodians and securely dispose of these assets. This will protect AI against security issues that can transfer from one AI system instantiation to another." (ETSI TS 104 223 [i.1])

Related threats/risks:

Improper disposal or transfer can lead to unauthorized data recovery, risking breaches, IP loss, and non-compliance with data protection laws.

Example Measures/Controls:

Develop and Implement a Secure Transfer and Disposal Policy with Data Custodian Oversight: Establish a comprehensive policy to govern the secure transfer and disposal of training data and models. Ensure that Data Custodians oversee all actions, confirming compliance with regulatory standards, protection of intellectual property, and adherence to organizational policies. This includes compliance with GDPR when involving personal data.

1.2.2. Provision 5.5.1-2

"If a Developer or System Operators decides to decommission a model and/or system, they shall involve Data Custodians and securely delete applicable data and configuration details." (ETSI TS 104 223 [i.1])

Related threats/risks:

Insecure data deletion during decommissioning can lead to unauthorized access to residual data, increasing regulatory and security risks.

Example Measures/Controls:

Implement a Secure Data Deletion Policy with Data Custodian Oversight: Establish a policy for securely deleting data and models during decommissioning, specifying methods compliant with standards. Ensure Data Custodians validate all deletions to maintain regulatory compliance and traceability.

2. Cloud Security Alliance (CSA)

2.1. AI Controls Matrix

Link: <https://cloudsecurityalliance.org/artifacts/ai-controls-matrix>

Link: <https://cloudsecurityalliance.org/artifacts/ai-controls-matrix>

2.1.1. DCS-01

Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually, or upon significant changes.

2.1.2. DCS-02

Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually, or upon significant changes.

2.1.3. DSP-02

Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.

3. Cyber Security Council (UAE)

3.1. National Cyber Security Policy for Artificial Intelligence

Link:

https://csc.gov.ae/documents/38662/0/National+Cyber+Security+Policy+for+Artificial+Intelligence_v1.1.pdf/4e02b32e-9f62-948d-4bc8-b580d596451b?t=1766994254544

Link:

https://csc.gov.ae/documents/38662/0/National+Cyber+Security+Policy+for+Artificial+Intelligence_v1.1.pdf/4e02b32e-9f62-948d-4bc8-b580d596451b?t=1766994254544

3.1.1. 3.2.1 Asset Management for AI/ML Systems - 5

The entity should have a process to decommission and securely dispose of AI/ML assets when they reach their end of life, ensuring that appropriate data is securely wiped and cannot be recovered.

4. CEN/CENELEC

4.1. prEN 40000-1-2: Cybersecurity requirements for products with digital elements - Part 1-2: Principles for cyber resilience

Link: <https://genorma.com/en/standards/pren-40000-1-2>

Link: <https://genorma.com/en/standards/pren-40000-1-2>

4.1.1. 7.10.

Planning for secure decommissioning

5. NCSC/NSA/CISA etc

5.1. AI Data Security

Link: https://media.defense.gov/2025/May/22/2003720601/-1/-1/0/CSI_AI_DATA_SECURITY.PDF

Link: https://media.defense.gov/2025/May/22/2003720601/-1/-1/0/CSI_AI_DATA_SECURITY.PDF

5.1.1. 1.9 Delete Data Securely

Prior to repurposing or decommissioning any functional drives used for AI data storage and processing, erase them using a secure deletion method such as cryptographic erase, block erase, or data overwrite. Refer to NIST SP 800-88, "Guidelines for Media Sanitization," [20] for guidance on appropriate deletion methods.

6. NIST

6.1. AI RMF 1.0

Link: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

Link: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

6.1.1. GOVERN 1.7

Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.